UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
DEPARTAMENTO DE CIENCIAS PENALES

El Rol de Agentes Policiales en la Investigación de Delitos Informáticos y Ciberdelitos

Memoria para optar al Grado de Licenciado en Ciencias Jurídicas y Sociales.

David Ignacio Durán Castelli
Profesor Guía: Profesor Ernesto Vásquez Barriga

Santiago, Chile
2023

Índice

Resumen:

El presente trabajo tiene como objeto analizar la forma en que actual e históricamente nuestros agentes policiales, carabineros y, más en específico, la Policía de Investigación (PDI), han participado en la investigación de delitos informáticos en su función de apoyo al Ministerio Público, y en general de los delitos que tienen como medio de comisión las nuevas tecnologías computacionales y el internet. Esto considerando las características de este tipo de delitos, definiéndolos y abordando sus características, con todas las especialidades que conllevan respectivamente, examinando entonces, cómo participan en la investigación de dichos delitos nuestros agentes policiales, revisando la normativa vigente relevante, doctrina y jurisprudencia pertinente. Dando cuenta así del rol investigativo de las policías en estos delitos, pasando por los importantes métodos de investigación criminalística utilizados por estas y los inéditos métodos que traen las nuevas tecnologías y legislación, al igual que incluir en la investigación la forma en que se aporta la prueba levantada mediante dichos métodos en juicio dentro del procedimiento penal, vislumbrando la jurisprudencia atingente, revisando la incidencia de la actuación policial y su prueba aportada, examinando la posible dificultad probatoria de este tipo de delitos para una eventual sentencia dictada, la información entregada a jueces para su debida comprensión, y finalmente en cuanto al tratamiento y valoración de la prueba por parte del juez para alcanzar los estándares probatorios.

Palabras Clave:

Delitos Informáticos - Cibercrimen - PDI - Investigación Criminal - Brigada Investigadora de Ciberdelitos - Carabineros

Introducción:

A raíz de la aparición de nuevas tecnologías y del avance en el uso de estas en el último tiempo, a través de su utilización, se vislumbran distintos delitos que han sido denominados “delitos informáticos” y otros tipos delictuales que comparten ciertas características con los anteriores, que corresponden al cibercrimen. En cuanto a los primeros, Chile mantuvo vigente la Ley 19.223 desde 1993, que tipifica únicamente cuatro tipos de delitos informáticos, con cierta amplitud que permitía su aplicación, pero que se volvía insuficiente y demasiado restringida en el contexto de las nuevas tecnologías, la modernidad y la internacionalización de estos aspectos, hasta que fue derogada en junio del año 2022, introduciendo así la Ley 21.459, con el objetivo de adecuar la legislación nacional a los estándares internacionales y, en específico, a los estándares propuestos por el Convenio de Budapest sobre delitos cibernéticos, de los cuales Chile es parte y ha suscrito.

No obstante, no serán los delitos informáticos propiamente tales los únicos a examinar, además son objeto de esta investigación, los delitos de explotación sexual a menores cometidos por internet, otros delitos contenidos en el Código Penal[1] que comparten características con los delitos informáticos, y todas las demás infracciones entendidas como delitos informáticos o ciberdelitos, por su especial contexto de tener como medio de comisión dispositivos informáticos y el internet, como pueden ser fraudes, estafas, robo de información, entre muchos otros, al presentar particularidades en cuanto a su investigación que son relevantes para comprender la participación policial en estos fenómenos.

Las diferencias en la naturaleza de este tipo de delitos, en comparación a los demás delitos comunes o que no tienen como medio las tecnologías y el internet, y en especial su característica de poseer no sólo la dimensión física sino que una virtual, hace que los delitos informáticos requieran de una especialización de las policías que sea adecuada, no solo de la legislación que los rige, sino que también de los métodos de investigación utilizados para lograr efectividad en las leyes y, en especial, la efectividad en la investigación.

En relación a la reciente modernización de la legislación de este tipo de delitos con la Ley 21.459, se hace necesario indagar cómo los nuevos tipos delictuales pueden afectar la investigación de aquellos por parte de los agentes policiales, en cuanto se

[1] Chile. *Código Penal,* artículo 411 y siguientes. 1874.

duplican los tipos penales de cuatro a ocho[2], por tanto, se diversifican los delitos, y aquello puede llegar a afectar la forma en que se investigan estos. Se debe agregar a lo anterior las múltiples dificultades que añade el medio para el delito, como la incidencia de la internacionalización de las investigaciones, ya que, debido a la globalización y la expansión del internet, los delitos cometidos en Chile pueden tener víctimas en todas partes del mundo, o pueden perpetrarse en el extranjero y tener víctimas en nuestro país.

Para la resolución de estos problemas relacionados a los medios de comisión de este tipo de delitos es que se creó una subdivisión especializada de nuestra Policía de Investigación dedicada a la exclusiva tarea de investigación especializada de dichos delitos, contando con los medios y herramientas específicas para levantar los respectivos insumos probatorios.

Es por todas estas razones que se escoge el tema presentado, siendo las nueva legislación respecto al tema, las especiales dificultades relativas a la investigación de este tipo de delitos, la especialización que ha tenido nuestra policía en cuanto a la forma en que se investigan y finalmente como la nueva legislación y la evolución de las tecnologías han afectado y probablemente afectarán su funcionamiento, y así lograr a través de este trabajo identificar el rol policial en la investigación de este tipo de delitos, y arribar satisfactoriamente a todos los objetivos que se presentan a continuación.

El objetivo de este trabajo es analizar y determinar cuál es el rol de los agentes policiales en los procedimientos relativos a delitos informáticos y al cibercrimen en general, y en específico, en cuanto a la investigación de aquellos, examinar cuáles son los métodos para su investigación, su eficacia, sus efectos e incidencia en los procedimientos llevados a cabo, por tanto, se busca identificar el rol de estos funcionarios y la eficacia de su actuación.

Como objetivos secundarios tendremos la determinación de los tipos penales que históricamente se han encontrado presentes en Chile, a partir de la Ley 19.223 y la nueva Ley 21.459 que deroga la anterior, los delitos relacionados a abuso de menores a través de internet y de los delitos que utilizan el internet como medio en general, y cómo ha entendido la doctrina sus características incluyendo en este punto la investigación general de los delitos cometidos a través de internet. En tercer lugar, se estudiará la metodología utilizada por nuestras policiales para investigar los delitos especiales denominados delitos informáticos al igual que su evolución y sus posibles cambios en

[2] Chile, *Ley N° 21.459*, 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos.

vista de la nueva legislación, determinar la eficacia de los métodos utilizados y analizar sus posibles efectos en los juicios que se lleven a cabo por la comisión de estos delitos.

Para determinar el rol de los agentes policiales respecto de los delitos informáticos, se estudiará el sistema penal chileno tanto en general, como también disponiendo especial atención a sus etapas, en las cuales los agentes policiales tienen incidencia como es la investigación, la producción de insumos probatorios, y la etapa de presentación de dichos insumos por parte de los agentes, que actúan como expertos o peritos; se analizarán los delitos informáticos, su tipificación, su historia y evolución y, debido a que se ha manifestado una modernización de este tipo de delitos, se analizarán también los cambios que trae la nueva legislación y las implicancias que tiene para la investigación y procedimiento penal en general. Se estudiarán las especialidades que tienen este tipo de delitos a la hora de ser investigados, los distintos métodos criminalísticos para producir insumos probatorios y cómo se comparan con el común de los delitos, analizando su eficacia y, por tanto, cómo los insumos probatorios levantados son presentados y posteriormente revisados, evaluados y valorados por los jueces en cuanto a su capacidad para probar los hechos relevantes.

En conjunto al punto anterior, se examinará la jurisprudencia relevante para lograr ejemplificar cómo han sido relevantes los trabajos de investigación y la evolución de sus métodos y técnicas para el procedimiento penal por delitos informáticos y de los demás delitos objeto de esta investigación. Por último, se dará importancia al estudio de jurisprudencia y experiencia comparada en cuanto a la investigación de los delitos informáticos, y los demás delitos investigados, para evaluar y comparar cómo se investigan y la relevancia de estas investigaciones en otros países con sistemas y reconocimiento similares a Chile, en conjunto con estudiar la participación de nuestras policías en las investigaciones de este tipo de delitos, cuando estos escapan de la sola jurisdicción nacional, y se requiere de cooperación internacional para su persecución.

Estos pasos son necesarios para determinar sus funciones, facultades y participación en general en el procedimiento penal por delitos informáticos, pero, además de estudiar estos aspectos en sí, es necesario determinar si estos ayudan a cumplir con los objetivos del sistema penal chileno.

Es un eje central de este trabajo la consideración de que las policías y sus actuales metodologías de investigación en delitos informáticos y del cibercrimen superan las dificultades que presenta un medio de comisión delictiva que evoluciona constantemente y que requiere de una especialización adecuada, logrando así una eficaz

aplicación de sus métodos para el levantamiento de insumos probatorios útiles para alcanzar el estándar probatorio necesario que responda con el objetivo de determinar con veracidad los hechos, y que además, han actuado eficazmente y de acuerdo a los estándares que se esperan en comparación a otros agentes de investigación a nivel internacional, al igual que en coordinación con otros agentes a nivel internacional cuando la investigación lo ha requerido.

Se requiere la comprensión de distintos fenómenos, conceptos y normas para un correcto análisis del funcionamiento de los agentes policiales al trabajar en casos de delitos informáticos y el cibercrimen, por lo que es necesario explicar las bases sobre las cuales se construye este trabajo.

Tanto en doctrina nacional como internacional el concepto de delito informático y sus tipos han sido estudiados y caracterizados, aunque en nuestra legislación su alcance ha sido restringido. Antes de la Ley 21.459, sólo poseíamos cuatro tipos penales relacionados a los delitos informáticos, los cuales se introdujeron en la Ley 19.223 de 1993, por lo que, a partir de ese punto, tanto la tecnología como la doctrina ha avanzado en cuanto al conocimiento y aplicación de este tipo de delitos.

Históricamente la doctrina ha entendido a los delitos informáticos como especiales, tipificados recientemente en la Ley 19.223. Esta ley establece cuatro delitos que protegen un bien jurídico en específico, entendiendo este, según explica Mario Garrido, como un elemento vital para la sociedad, o para un individuo, que debe ser protegido, con distintas matices y definiciones, que puede incluir o no elementos históricos, culturales, etc.[3], aquello se desprende de la moción de Ley cuando esta fue promulgada, siendo la "calidad, pureza, idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan"[4], y además, una serie de otros bienes jurídicos, debiendo entender estos como delitos pluriofensivos, como así lo ha entendido Eric Chávez[5].

Se entiende por este tipo de delitos los contenidos actualmente en la Ley 21.459, que tipifica específicamente ocho tipos penales respecto de los cuales, si bien nuestra doctrina nacional se ha hecho cargo del estudio de los cuatro que se mantienen a partir

[3] GARRIDO MONTT, Mario. "*Derecho Penal. Parte General. Tomo I*". Chile: Editorial Jurídica de Chile, 2010. Pgs 63-68. Disponible en: Vlex Chile

[4] Chile, Congreso Nacional. *Moción Parlamentaria de Ley N° 19.223*, 16 de julio de 1991, Legislatura número 322, página 1. Disponible en Historia de la Ley N° 19.223.

[5] CHÁVEZ CHÁVEZ, Eric Andrés. "Décimo Grupo: Delitos Contenidos en Leyes Especiales". En: *Derecho Penal, Parte Especial*. Primera Edición. Tofulex, ediciones jurídicas. 2019. pp 709-713. Disponible en: Vlex Chile.

de la Ley 19.223, los demás pueden ser asimilables o son debidamente analizados a raíz de la doctrina internacional, entendiendo que la legislación vigente, nace a partir de la necesidad de adecuarse precisamente a Convenios Internacionales acerca del tema, en específico al Convenio de Budapest, tal y como lo establece la Ley 21.459.[6]

El delito informático no se encuentra totalmente definido por la doctrina, sino que describe distintos fenómenos delictuales, como explica José Cuervo, en nuestro país estos delitos corresponden a aquellos en los cuales el objeto ilícito dice relación con el uso de sistemas de tratamiento de información, o los comúnmente utilizados para este objetivo como las computadoras o teléfonos celulares, además pueden ser aquellos delitos que utilizan estos sistemas como el medio para la comisión de delitos[7].

Los tipos delictuales que serán sujetos de una parte de la investigación son los contenidos en la Ley 19.223, los cuales han sido definidos y estudiados por la doctrina, entendiéndose dos tipos de delitos, sabotaje informático y espionaje informático. Como lo ha entendido la doctrina, los artículos 1º y 3º corresponden a sabotaje, mientras que el 2º y el 4º artículo corresponden a espionaje. Sabotaje se entiende como un delito que tiene como objeto los sistemas de tratamiento de información, tanto en su dimensión física como digital, o los datos contenidos dentro de estos, y los delitos de espionaje, que dicen relación con la intención maliciosa y uso indebido de datos e información obtenidos de los sistemas informáticos.[8]

Actualmente, los delitos informáticos tipificados se encuentran en la Ley 21.459, que establece la captación de información sin consentimiento, la difusión de dichas información, la producción de programas o dispositivos para los objetivos anteriormente mencionados, la difusión de información de un sistema informático (diferente de un dispositivo), el uso y manipulación de claves o contraseñas y datos sensibles relativos a tarjetas comerciales, la aplicación de programas para la valoración de integridad de datos, la alteración o daño de sistemas informáticos y, por último, la alteración de datos para obtener acceso a un sistema informático.[9]

Por supuesto, los delitos informáticos o ciberdelitos no se limitan a los contenidos en dicha legislación, pues se deben considerar como tal todos los delitos que tienen

---

[6] Chile, Congreso Nacional. *Ley N° 21.459*, 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos.
[7] CUERVO ÁLVAREZ, José. "*Delitos informáticos: Protección Penal de la Intimidad"*. España. 2014. Disponible en: Delitos informáticos: Protección Penal de la Intimidad.
[8] CHÁVEZ CHÁVEZ, Eric Andrés. Ob. Cit. pp 709-713. Disponible en: Vlex Chile.
[9] CAMPOS, Rodrigo "*Capítulo II Normativa aplicable a los servicios de Cloud Computing utilizados por la administración del Estado*". En: Jejina, Renato. *Derecho Informático*, 1era edición, Santiago, Chile: Editorial El Jurista, 2022. P. 299-301.

como medio para la comisión del delito tanto el internet como los dispositivos que manejan información, como también las modificaciones introducidas por la Ley 19.927 al Código Penal en cuanto delitos de pornografía infantil.

La doctrina internacional es más extensa en cuanto a los tipos delictuales que la anterior Ley 19.223, la cual fue insuficiente para describir la multiplicidad de formas en las que pueden cometerse delitos de este tipo, tanto utilizando medios informáticos como a través de internet.[10] En vista de la nueva legislación y su objetivo, debemos indicar que se han hecho limitados estudios de la actual legislación, y que en su gran mayoría se presentan estudios e investigaciones respecto al contenido y aplicación de la Ley 19.223. La doctrina internacional en algunos casos posee igualmente mayor extensión de delitos que la nueva Ley 21.459.

Para la investigación de este tipo de delitos nuestras policías poseen una brigada especializada que se encarga de todos los aspectos relacionados a delitos informáticos y, en general a todo tipo de cibercrimen, denominadas las Brigadas Investigadoras del Cibercrimen, pertenecientes a las Policías de Investigación, que tal y como establece el sitio web de la PDI[11], investiga delitos informáticos, delitos relacionados a la explotación sexual de menores a través de internet, y en general, delitos que utilicen la tecnología y el internet como medio de comisión.

Igualmente, para la investigación de los delitos antes mencionados, nuestras policías cuentan con todos los medios que les entrega nuestro Código Procesal Penal, pero la Ley 21.459 específica las herramientas que deben ser utilizadas a la hora de la investigación. Esta, en su artículo 12º, expresa que en la investigación de los delitos contenidos en la Ley se deben utilizar especialmente los métodos de investigación contenidos en los artículos 220 a 226 del Código Procesal Penal en cuanto a la interceptación de comunicaciones telefónicas o de otras formas de telecomunicación, como pueden ser las redes del internet. Además de lo anterior, la Ley añade un nuevo método para la investigación, introduciendo la figura del Agente Encubierto[12], de las formas en que se pueden llevar a cabo las diligencias antes mencionadas, al igual que las herramientas y tecnologías utilizadas para la producción de insumos probatorios, su cuidado, almacenamiento, y posterior análisis investigativo son elementos que el Ministerio Público y los cuerpos policiales deben realizar.

---

[10] NARVAEZ, David. *El delito informático y su clasificación*, UNIANDES, Revista de Ciencia, Tecnología e Innovación, 2015, Vol. 2, Número 2, p. 158-173. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6756355.pdf

[11] *Cibercrimen*, Policía de Investigaciones, 2020. Disponible en: Brigadas Investigadoras del Cibercrimen.

[12] Chile, Congreso Nacional *Ley N° 21.459*, 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos

Capítulo 1: El sistema Penal y el Rol Policial

Para la adecuada comprensión del rol de los policías en el sistema penal chileno primero debemos definir las características de este, y principalmente, presentar sus etapas y la incidencia de los agentes policiales en cada una de estas, debido a que las actuaciones de las policías y su participación en un procedimiento penal dependerán de cuál sea la fase en la que están actuando, desde la investigación, hasta la aprehensión de individuos y la asistencia en juicios.

El sistema penal chileno corresponde a un sistema adversarial y acusatorio, con una base en la separación de las funciones de acusación e investigación, defensa y por último en quien juzga al acusado[13]. Que sea un sistema acusatorio se denota en diversos aspectos, como por ejemplo, el inicio del proceso se lleva a cabo por un ciudadano o un órgano distinto del juez, que puede ser, entre otros, el Ministerio Público, también se denota toda vez que el procedimiento es público, oral, que existe igualdad entre las partes ante el juez y durante la totalidad del procedimiento[14], es este el tipo de proceso que se tiene en Chile, con algunas modificaciones y cambios, y es alrededor de este tipo de sistema donde las policías cumplen sus distintas funciones.

En primer lugar, la investigación depende del Ministerio Público y es este quien cumple la función investigadora y de eventual acusación dentro del procedimiento penal de cualquier delito sobre el cual tome conocimiento, así lo indica el artículo 77 del código Procesal Penal[15]. Para esto, designa un fiscal que estará a cargo de cada caso en específico, el cual tiene como función representar al Ministerio Público ante los tribunales penales, al igual que estar a cargo de la investigación del caso, utilizando todos los recursos y herramientas que le entrega la Ley.

Los pasos y formas en que el Ministerio Público lleva a cabo su tarea dependen del momento en el proceso en el que se está actuando, incluyendo entonces, dentro de sus actuaciones, las tareas que los agentes policiales tengan dentro del procedimiento. Pero para determinar estas últimas, primero debemos indicar cuales son las etapas del procedimiento penal en el sistema penal acusatorio chileno y analizar dentro de cada una de estas la incidencia de los agentes policiales.

---

[13] NUÑEZ VÁZQUEZ, J. Cristóbal. "*Tratado del Proceso Penal y del juicio oral*". Tomo I. Chile. Editorial Jurídica de Chile. 2009. p. 21. Disponible en: Vlex Chile

[14] MATURANA MIQUEL; MONTERO, Cristián; LÓPEZ, Raúl. *Derecho Procesal Penal. Tomo I*. 1° edición. Chile. Abeledo Perrot Legal Publishing. p. 92

[15] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 77. 2000.

1.1 Etapas del procedimiento penal:

Cabe mencionar que, como el objetivo del sistema penal acusatorio es principalmente la búsqueda de la verdad, la determinación correcta de los hechos y la entrega de una respuesta eficaz frente a los delitos, son de suma importancia muchas de las labores que realizan las policías durante el procedimiento, las que serán explicadas a continuación. Cabe mencionar, de todas formas, que los objetivos del sistema penal y del procedimiento penal siempre se expresan con pleno derecho a las garantías de los intervinientes, solucionando finalmente el conflicto entre el *ius puniendi* y el derecho de libertad o a la libertad del imputado[16].

Durante el procedimiento penal no siempre tienen incidencia los agentes policiales. Sin embargo, es importante explicar cuáles son dichas etapas y en qué consisten, además de demostrar cómo los agentes policiales intervienen y participan en cada una de ellas.

Las etapas del procedimiento penal chileno son las siguientes:

1. Inicio del procedimiento: El procedimiento penal chileno comienza con la investigación por parte de la fiscalía sobre hechos que pueden revestir la calidad de delito, a través de la denuncia, de la querella, o de oficio por parte del ministerio público. Una vez la fiscalía tenga los antecedentes suficientes, y si decide que los hechos revisados revisten la calidad de delito, se procede a realizar la formalización del imputado, la cual se concreta en la audiencia de formalización. Esta es una fase meramente escrita en lo que concierne a la acusación en sí, sin olvidar que el procedimiento penal se rige por el principio de oralidad.

   No es sino cuando se cumplen estos pasos previos que la fiscalía procederá a la acusación del imputado respecto del delito por el cual se le acusa. Si los hechos no revisten calidad de delito o si posteriormente durante la investigación los antecedentes y hechos investigados no constituyen delito, no se realizará acusación de este, debiendo realizarse el sobreseimiento definitivo, distinto es el caso de las salidas alternativas al procedimiento que se revisarán posteriormente en este trabajo.

[16] NUÑEZ VÁZQUEZ, J. Cristóbal. "*Tratado del Proceso Penal y del juicio oral*". s.n. Tomo I. Chile. Editorial Jurídica de las Américas. 2009. pp. 9-14. Disponible en: Vlex Chile

El inicio del procedimiento está dictado por el artículo 172 del Código de Procedimiento penal, que indica: "*Formas de inicio. La investigación de un hecho que revistiere caracteres de delito podrá iniciarse de oficio por el ministerio público, por denuncia o por querella.*"[17]

En cuanto al accionar policial, esta etapa da entonces a los agentes policiales la capacidad para comenzar con las investigaciones correspondientes que nos llevarán al levantamiento de insumos probatorios, lo cual es una de las funciones principales de los agentes policiales en el procedimiento penal y lo que será objeto de gran parte de este trabajo de investigación. Se entiende como parte de esta etapa del procedimiento las labores de detención que efectúan carabineros, fuerzas especiales o policías de investigación, y la formulación de medios probatorios a través de la toma de declaraciones, el cuidado del sitio del suceso, y la recepción de la prueba en este.

Dichas actuaciones pueden verse descritas en el artículo 83 del Código Procesal Penal:

"Actuaciones de la policía sin orden previa. Corresponderá a los funcionarios de Carabineros de Chile y de la Policía de Investigaciones de Chile realizar las siguientes actuaciones, sin necesidad de recibir previamente instrucciones particulares de los fiscales:

a) Prestar auxilio a la víctima;

b) Practicar la detención en los casos de flagrancia, conforme a la ley;

c) Resguardar el sitio del suceso. Deberán preservar siempre todos los lugares donde se hubiere cometido un delito o se encontraren señales o evidencias de su perpetración, fueren éstos abiertos o cerrados, públicos o privados. Para el cumplimiento de este deber, procederán a su inmediata clausura o aislamiento, impedirán el acceso a toda persona ajena a la investigación y evitarán que se alteren, modifiquen o borren de cualquier forma los rastros o vestigios del hecho, o que se remuevan o trasladen los instrumentos usados para llevarlo a cabo.

El personal policial experto deberá recoger, identificar y conservar bajo sello los objetos, documentos o instrumentos de cualquier clase que parecieren haber servido a la comisión del hecho investigado, sus efectos o los que pudieren

[17] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 172. 2000

ser utilizados como medios de prueba, para ser remitidos a quien correspondiere, dejando constancia, en el registro que se levantare, de la individualización completa del o los funcionarios policiales que llevaren a cabo esta diligencia;

En aquellos casos en que en la localidad donde ocurrieren los hechos no exista personal policial experto y la evidencia pueda desaparecer, el personal policial que hubiese llegado al sitio del suceso deberá recogerla y guardarla en los términos indicados en el párrafo precedente y hacer entrega de ella al Ministerio Público, a la mayor brevedad posible.

En el caso de delitos flagrantes cometidos en zonas rurales o de difícil acceso, la policía deberá practicar de inmediato las primeras diligencias de investigación pertinentes, dando cuenta al fiscal que corresponda de lo hecho, a la mayor brevedad. Asimismo, el personal policial realizará siempre las diligencias señaladas en la presente letra cuando reciba denuncias conforme a lo señalado en la letra e) de este artículo y dará cuenta al fiscal que corresponda inmediatamente después de realizarlas. Lo anterior tendrá lugar sólo respecto de los delitos que determine el Ministerio Público a través de las instrucciones generales a que se refiere el artículo 87. En dichas instrucciones podrá limitarse esta facultad cuando se tratare de denuncias relativas a hechos lejanos en el tiempo.

d) Identificar a los testigos y consignar las declaraciones que éstos prestaren voluntariamente, en los casos de delitos flagrantes, en que se esté resguardando el sitio del suceso, o cuando se haya recibido una denuncia en los términos de la letra b) de este artículo. Fuera de los casos anteriores, los funcionarios policiales deberán consignar siempre las declaraciones que voluntariamente presten testigos sobre la comisión de un delito o de sus partícipes o sobre cualquier otro antecedente que resulte útil para el esclarecimiento de un delito y la determinación de sus autores y partícipes, debiendo comunicar o remitir a la brevedad dicha información al Ministerio Público, todo lo anterior de acuerdo con las instrucciones generales que dicte el Fiscal Nacional según lo dispuesto en el artículo 87;

e) Recibir las denuncias del público, y

f) Efectuar las demás actuaciones que dispusieren otros cuerpos legales"[18]

[18] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 83. 2000

Realizada la audiencia de formalización en la cual se le informa al imputado la investigación en su contra, además de los aspectos antes mencionados, se establecen aspectos como las medidas cautelares.

2. Etapa de investigación: Le corresponde al Ministerio Público llevar a cabo la producción de insumos probatorios de forma previa a la acusación al imputado. Una vez terminada la obtención de la prueba, se termina la fase de investigación y se da apertura e inicio a la fase de preparación del juicio oral[19]. Esta fase del procedimiento tiene dos partes, la investigación desformalizada y la investigación formalizada.

a. Fase de investigación desformalizada: Realizada por el Ministerio Público. En esta etapa se recopilan todos los antecedentes que no producen efectos jurídicos y que, por tanto, no tienen valor probatorio por no rendirse en el juicio oral, pero pueden adquirir esta condición posteriormente, una vez son presentadas y aceptadas como medio de prueba al hacerse valer en el procedimiento, en el juicio. La investigación no se formaliza hasta que se requiera efectuar alguna diligencia que afecte los derechos o garantías del imputado.

b. Fase de investigación formalizada: Efectuada la formalización por el fiscal a cargo, comienza a correr el plazo de investigación, y las diligencias de presentación de los resultados de dicha investigación es parte del procedimiento ya iniciado, presentando los insumos probatorios en la audiencia de apertura del juicio oral, pero solo a modo de ofrecimiento de esta, para determinar su validez y legalidad.

Como ya se dijo, esta parte contiene la fase de investigación formalizada, la cual es la etapa más importante para este trabajo de investigación, debido a que es donde las policías producen insumos probatorios, para lo cual se requieren diferentes técnicas y grupos de especialización dentro de los distintos cuerpos policiales, como lo son Carabineros de Chile, y en especial, nuestra Policía de Investigación (en adelante PDI). Estas utilizan técnicas científicas y de otros tipos para la investigación de los hechos, para poder finalmente levantar insumos probatorios que ayuden al Ministerio Público a dar la respuesta correcta al caso concreto y a discernir la verdad, en función de que este último debe mantenerse en sujeción al principio de objetividad, bajo el cual el artículo 77 del Código

[19] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 259. 2000

Procesal Penal establece que "*Facultades. Los fiscales ejercerán y sustentarán la acción penal pública en la forma prevista por la ley. Con ese propósito practicarán todas las diligencias que fueren conducentes al éxito de la investigación y dirigirán la actuación de la policía, con estricta sujeción al principio de objetividad consagrado en la Ley Orgánica Constitucional del Ministerio Público.*"[20].

Respecto a la incidencia policial en esta etapa, el levantamiento de insumos probatorios es el objeto principal de este trabajo de investigación, debido a que el objeto estudiado -los delitos informáticos-, presentan particularidades a la hora de ser debidamente investigados, requiriendo un mayor grado de especialización por parte de los agentes investigadores. Los delitos informáticos son ahora delitos altamente específicos, donde se requiere además que la evidencia que sea recopilada tenga las características y capacidades para ser utilizadas dentro del procedimiento.

3. Etapa Intermedia: Esta etapa comienza con la acusación por parte del Ministerio Público, celebrándose dentro de esta etapa la audiencia preparatoria del juicio oral. Las audiencias orales celebradas durante esta etapa tienen por finalidad determinar el objeto del juicio y en especial determinar las pruebas que se rendirán en la siguiente etapa del procedimiento, entre otras finalidades que no serán objeto de estudio. Siendo crucial en esta etapa la audiencia de preparación del juicio oral, en la cual se depura la prueba y se admite o rechaza para ser valorada en un juicio oral.

La incidencia policial en esta etapa del procedimiento penal es relevante para la investigación, toda vez que la eficacia de la prueba presentada en el procedimiento dependerá de la calidad de la labor realizada por los funcionarios encargados de dicha tarea.

4. Etapa de juicio oral: Esta etapa es eventual y corresponde al período de audiencias orales que ocurren una vez la etapa de investigación formalizada haya finalizado, se lleva ante el tribunal oral y tiene por finalidad determinar la sentencia final.

Durante esta etapa la participación de las policías es relevante para el procedimiento, no así para el objetivo de este trabajo, con la excepción de la participación de agentes policiales que aportan al proceso como expertos y

[20] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 77. 2000

peritos, para contribuir a través de su experticia al esclarecimiento de factores técnicos y la aportación de prueba especializada, lo cual es especialmente relevante dada la complejidad que adquiere la prueba y los métodos para conseguirla, por lo que se vuelve necesario la especialización de los funcionarios policiales.

Es también en esta etapa donde se presenta la prueba recabada por los agentes policiales y el ministerio público, habiendo pasado las barreras de validez y legalidad de la audiencia de apertura del juicio oral.

5. Salidas Alternativas y otras formas de conclusión del procedimiento: Cabe mencionar que el código de procedimiento penal menciona dos formas de salida alternativa al procedimiento penal, siendo estas la suspensión condicional del procedimiento y los acuerdos reparatorios[21], donde la labor de las policías en la investigación de los delitos pueden llegar a ser relevantes o importantes para que se llegue o se decida optar por estas salidas alternativas.

A lo anterior debe agregarse los casos del procedimiento abreviado, que corresponde a aquellos en los que no existe controversia acerca de los hechos investigados y probados por la fiscalía, donde es de vital importancia la investigación realizada por las policías, toda vez que pueden llegar a conducir a este tipo de procedimientos. Por último, cabe mencionar respecto del procedimiento simplificado, donde es esencial la investigación de las policías, debido a que es en la etapa de investigación donde la fiscalía determinará la posibilidad y factibilidad de aplicación de estos tipos de procedimientos[22].

Teniendo bajo conocimiento cuáles son las etapas que componen el procedimiento penal del sistema penal acusatorio chileno, y de igual forma cómo participan nuestros agentes policiales en cada una de las etapas atendiendo a las tareas que se les imponen, debemos entonces determinar a continuación cómo se desarrollan estas labores y sus efectos dentro del procedimiento penal. Dichas laborales son las de investigación en las etapas respectivas y las de producción de insumos probatorios, en

---

[21] DUCE, Mauricio. "*Salidas alternativas o formas alternativas de resolución del conflicto en el proceso penal*". En: DUCE, Mauricio y RIEGO, Cristián. "*Proceso Penal*". s.n. Chile. Editorial Jurídica de las Américas. 2009. pp. 306-320. Disponible en: Vlex Chile

[22] HORVITZ LENNON, María Inés y LÓPEZ MASLE, Julián. "*Derecho Procesal Penal Chileno II. Preparación del juicio, procedimientos especiales, ejecución de sentencias, acción civil*". s.n. Chile. Editorial Jurídica de las Américas. 2008. pp. 503-508. Disponible en: Vlex Chile

conjunto a la participación como testigo experto y como perito cuando corresponda, las únicas que son objeto de este trabajo de estudio, para determinar en qué consisten, cómo se encuentran normadas y cómo se desarrollan en el procedimiento.

1.2 La función de investigación:

La investigación se encuentra a cargo del Ministerio Público, que, mediante los fiscales, tienen a su disposición a las policías para llevar a cabo sus labores. Esto ya que como se establece en el Código Procesal Penal en su artículo 79, las fuerzas de Orden y seguridad pública deben ser un apoyo al Ministerio Público en su labor de investigación, entonces el Ministerio Público hace uso de las fuerzas policiales para llevar a cabo la investigación de los delitos para levantar insumos probatorios[23]. Estos son los elementos de los cuales dispone el Ministerio Público para presentar durante el juicio penal como evidencias. No es solo Carabineros y la PDI quienes pueden participar de la investigación, sino que en casos donde se requiera, las fuerzas de Gendarmería pueden llegar a participar de la investigación.[24]

Para llevar a efecto la labor de investigación, se otorga a las policías[25] distintas herramientas dispuestas en el Código Procesal Penal, al igual que en leyes para delitos especiales, por lo tanto, estas provienen de la ley. Aun así, los artículos y leyes que proponen las herramientas de investigación lo hacen de forma general, en el sentido en que los métodos, técnicas, experticias y tecnologías que pueden ser utilizadas para los fines propuestos varían inmensamente, por lo que las policías mantienen una variedad de métodos de investigación que pueden llegar a ser altamente específicos y especializados dependiendo del tipo de delito y su medio de comisión.

Con el objetivo de lograr una adecuada producción de insumos probatorios contamos con dos policías, Carabineros de Chile y la Policía de Investigaciones (PDI), de los cuales la ley en este ámbito no diferencia sus funciones y en específico, ambas comparten la tarea de apoyo en la investigación en conjunto al ministerio público, así se establece en el Código Procesal Penal.[26]

Es el fiscal a cargo de la investigación quien, a través de sus instrucciones determina cuál de las policías llevará a efecto el total o parte de las labores de investigación, por lo tanto, no solo Carabineros realiza esta labor, sino que debemos

[23] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 79. 2000
[24] Ibídem.
[25] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 3. 2000
[26] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 79. 2000

destacar la labor de la PDI, una policía especializada que tiene como principal función la investigación de delitos, la cual posee herramientas y capacidades de investigación específicas y efectivas. Además de herramientas propias de la labor investigativa, la PDI tiene subdivisiones para materializar su labor desde distintos ángulos y separar sus funciones respecto a especialidad y área de manejo en cuanto a la investigación, existiendo ramas y áreas dentro de esta que no solo se enfocan al ámbito de la investigación de un mismo delito en forma conjunta, sino que se separan para la investigación de ilícitos en específico que requieren de un mayor grado de especialización, como por ejemplo los delitos económicos, delitos relacionados a la migración, la interpol, entre otros. Pero cabe destacar para este trabajo de investigación, la existencia de las Brigadas Investigadoras del Cibercrimen, que tienen como función la investigación de los delitos informáticos, apoyar en la investigación de delitos que tienen como medios de comisión sistemas informáticos y en general las redes de internet.

En esta línea, cabe indicar que son funciones exclusivas de la policía en materia de investigación del delito las contenidas en los artículos 180, 181 y 187 del Código Procesal Penal, entre estas identificar a los partícipes del delito, la constatación de las personas, cosas y lugares afectados por los actos, levantar los indicios como huellas o rastros, y en general todas aquellas diligencias que tengan relación a estas labores.

En su actuar, todas las diligencias producidas por las policías tienen carácter de reservados y deben ser debidamente informadas al fiscal, al igual que deben dejar registro de todas estas diligencias. Estas son las funciones de los agentes policiales en general, que serán revisadas en específico más adelante.

1.2.1 De Carabineros en General:

Carabineros es la principal policía en nuestro País, es un cuerpo policial armado no deliberante, profesional, jerarquizado y disciplinado, que tiene como principal función la protección del orden público y la prevención del delito, así lo ha entendido la doctrina[27]. Esto último tiene especial relevancia para el procedimiento penal, ya que son quienes detienen a los imputados de un ilícito penal cuando así lo estima pertinente el tribunal a petición del Ministerio Público, además de tener la obligación de realizarlo cuando el delito es cometido en flagrancia[28], esto último incluye igualmente a la Policía de investigaciones, al ser también agentes policiales.

---

[27] MATURANA MIQUEL; MONTERO, Cristián; LÓPEZ, Raúl. *Derecho Procesal Penal. Tomo I*. 1° edición. Chile. Abeledo Perrot Legal Publishing. p. 228

[28] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 125 a 129. 2000

Esta institución fue creada en 1927, se encuentran especialmente regulados en la Ley 18.961, sus labores de investigación se encuentran establecidas en el artículo 79 de dicha Ley, imponiendo su función de ayuda al Ministerio Público, y en específico, de las funciones de la rama de la Policía de investigación.

Como se mencionó anteriormente, Carabineros cumple distintas funciones en nuestra sociedad, pero las relevantes para este trabajo dice relación con las actuaciones que realizan en su función de auxiliares del Ministerio Público, para ello tienen a su disposición laboratorios y organismos especializados de los cuales pueden hacer uso para estas labores[29]. Además de esto, Carabineros cumple funciones dentro del procedimiento que no dependen del fiscal a cargo o del Ministerio Público[30], al igual que prestar asistencia a los órganos judiciales cuando estos lo requieran.

Estas son las actuaciones y facultades, relevantes para este trabajo de investigación, que realiza Carabineros, en cuanto a su participación activa dentro de las diferentes etapas del procedimiento penal. Como se dilucidó, Carabineros actúa en gran parte de las etapas del proceso, desde su inicio hasta su fin, con funciones más o menos relevantes para este trabajo, aunque cabe mencionar sus funciones relativas al almacenamiento, traslado y análisis de evidencias y materiales relacionados y relevantes para la investigación de todo tipo de delitos, en específico de los que serán estudiados en este trabajo.

1.2.2 De la Policía de Investigaciones en General:

La Policía de Investigaciones de Chile o PDI es una institución policial cuyo marco legal se encuentra contenido en su propia ley, la Ley Orgánica de la Policía de Investigaciones de Chile, en donde se describe su principal función la cual es la de investigar los delitos[31], y sus demás funciones, entre las cuales podemos apreciar una superposición con las labores de carabineros, que se encuentran en el artículo 4to de su Ley orgánica antes nombrada.

Para llevar a cabo su principal función, la PDI se separa en brigadas especializadas según el tipo de delito investigado, dependiendo estas de la Jefatura

[29] Chile. Congreso Nacional. Artículo 3° *Ley orgánica Constitucional de Carabineros* 18.961 de 7 de marzo de 1990.
[30] Chile. Congreso Nacional. Artículo 4° *Ley orgánica Constitucional de Carabineros* 18.961 de 7 de marzo de 1990.
[31] Chile. Congreso Nacional. Artículo 4° *Decreto Ley 2460* del 9 de enero de 1979.

Nacional de la PDI[32]. Estas brigadas o ramas de la policía tienen distintos recursos y laboratorios a su disposición, pero pueden trabajar conjuntamente si así es necesario.

Entre las brigadas de la PDI, serán objeto de estudio la Brigada de Investigación de Cibercrimen, que dentro de sus objetivos se encuentra la investigación de los delitos informáticos, para lo cual esta posee policías que se han especializado para la investigación de este tipo de delitos y de todo tipo de delitos que tengan como medio de comisión el internet y los sistemas informáticos en general, contando con las herramientas necesarias para superar las dificultades que vienen de la mano con estos medios de comisión.

1.2.3 La participación como testigo experto o perito:

Otra forma en que las policías pueden participar en el procedimiento penal es como testigos expertos o peritos, de esta forma se presentan ante el tribunal a dar testimonio, prestando su opinión experta o declarando sobre lo detallado en sus informes periciales que se añaden a la prueba presentada en el juicio por el Ministerio Público por medio de la declaración. Como mencionamos anteriormente, los agentes policiales pueden alcanzar un alto grado de especialización, adquiriendo conocimientos y profesionalizándose en estos, lo cual presenta un gran aporte toda vez que los delitos de los cuales trata un juicio pueden requerir de conocimientos técnicos fuera de las capacidades de un tribunal. Esto es especialmente importante en los delitos estudiados, comprendiendo que los delitos informáticos conllevan tecnicismos y que el análisis de su medio de comisión requiere de un experto en los temas relacionados para poner en conocimiento al tribunal y ser un aporte para el esclarecimiento de los hechos.

Esta función se encuentra contenida en el Código Procesal Penal[33] y sigue las reglas establecidas para los testigos y peritos. Estos peritos presentados por el Ministerio Público pueden pertenecer a cualquier rama o subdivisión de los órganos policiales, y se hará uso de este recurso dependiendo del área de experticia, pertenencia a un laboratorio u organismo especializado de los órganos que presten auxilio al Ministerio Público en su labor de investigación.

---

[32] MATURANA MIQUEL; MONTERO, Cristián; LÓPEZ, Raúl. *Derecho Procesal Penal. Tomo I*. 1° edición. Chile. Abeledo Perrot Legal Publishing. p. 231.
[33] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 321. 2000

Esta función que pueden cumplir los agentes policiales puede llegar a ser especialmente relevante y se volverá a revisar más adelante en esta investigación debido a la especialización requerida para la investigación de este tipo de delitos con un medio de comisión tan complejo como el presentado.

Por tanto, puede llegar a ser importante el apoyo en forma de perito experto en temas informáticos y digitales por parte de un funcionario policial, en general, explica así Mauricio Duce que el ejercicio de la pericia como opinión de un funcionario experto es una práctica importante y común para la investigación y presentación en juicio[34], que puede ayudar al juez a comprender las dificultades y particularidades, al igual que los tecnicismos propios correspondientes al cibercrimen y los delitos informáticos.

[34] DUCE J. Mauricio. "*Una aproximación empírica al uso y prácticas de la prueba pericial en el proceso penal chileno a la luz de su impacto en los errores del sistema*". en Política Criminal. s.n. p. 43. Disponible en Vlex Chile

Capítulo 2: Tratamiento Histórico de los delitos informáticos y el cibercrimen en Chile:

A través de la historia legislativa de Chile los delitos informáticos han tenido un limitado tratamiento legislativo, poseyendo hasta la actualidad únicamente dos leyes que los tratan en específico, incluyendo dentro de estos otros tipos de delitos que tienen como medio de comisión exclusivo el internet o los sistemas informáticos asociados, habiendo entonces una limitada gama de leyes que regulan estos temas.

La legislación últimamente ha sido actualizada y expandida a raíz de los estándares internacionales[35], y de esto debemos destacar que, en cuanto al cibercrimen, estos delitos tienen diferencia en su medio de comisión, más no específicamente en el delito en sí, por lo que provienen de delitos ya reconocidos por el Código Penal que tienen una modalidad digital, o de delitos especiales que no son parte de los Delitos Informáticos de sus respectivas leyes.

2.1 Ley 19.223 de sobre Delitos Informáticos:

La ley que se mantuvo vigente por la mayoría de la historia de Chile es la Ley 19.223 promulgada en el año 1993, en la cual solo se consideraron cuatro figuras delictivas, lo cual limitó el tratamiento que tuvieron este tipo de delitos con una baja cantidad de figuras, las cuales son especialmente restrictivas, no atendiendo a la necesidad de apertura al cambio y a los avances tecnológicos que requiere la materia, sin tener cambios a dicha ley hasta el año 2022. Los delitos contenidos en dicha Ley se pueden clasificar de la siguiente forma:

a) Sabotaje: El sabotaje se entiende como los delitos que tienen como objeto los sistemas de tratamiento de información, tanto en su dimensión física como digital, o los datos contenidos dentro de estos, y lo que se prescribe es el acto de destruirlos o afectarlos, modificándolos o impidiendo su funcionamiento o el de cualquiera de sus partes o datos. Corresponden a esta clasificación de delitos los contenidos en los artículos número 1º y 3º de la Ley 19.223.

b) Espionaje: El espionaje hace referencia a los delitos que dicen relación con una intención maliciosa de uso indebido de los datos y la información

[35] Chile, Congreso Nacional. *Ley N° 21.459*, 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos

contenida en los sistemas informáticos afectos, incluyendo la forma en que se obtienen dichos datos, considerando que esta puede ser de manera maliciosa o buscar el uso indebido proscrito y la eventual difusión, y los posibles objetivos dañinos que puede tener dicha difusión de los datos. Como describe Eric Chávez, los artículos que contienen este tipo de delitos son los números 2º y 4º de la Ley 19.223.[36]

Con esta clasificación de los delitos informáticos, tratados en la Ley 19.223, podemos ver que se tiene una limitada cantidad delitos, siendo solo cuatro. Pero a este conjunto de delitos se les puede añadir una limitada cantidad de legislación que trata delitos que tienen como medio de comisión el internet y los sistemas informáticos o se consideran como cibercrimen.

2.2 Ley 19.927 que modifica los artículos sobre delitos relaciones a la pornografía Infantil:

Otra de las leyes que tienen como figura específica una relacionada al medio de comisión internet es la Ley 19.927, que añade al código penal las figuras de posesión de pornografía infantil y sobre su producción a través de internet[37]. Es importante añadir este tipo de delitos toda vez que su forma de comisión exclusiva es el internet, entendiendo que el delito de posesión y el de producción de pornografía infantil pueden tener como medio de comisión el plano físico y no así el digital, se ha añadido especialmente la figura que tiene como medio de comisión el internet.

Esta legislación expande las figuras delictivas de posesión de pornografía infantil, producción de esta, la exhibición de material sexual a menores, entre otros, y los extiende para cubrir la dimensión digital de este tipo de delitos, al igual que expandir la forma en que estos pueden ser investigados, a través de la interceptación de comunicaciones por medios digitales, entre otros. Igualmente se expande el delito de comercialización, distribución y exhibición de este tipo de materiales cuando tengan por medio cualquier tipo de telecomunicaciones, lo cual cabe dentro de los medios como el internet.[38]

---

[36] CHÁVEZ CHÁVEZ, Eric Andrés. “Décimo Grupo: Delitos Contenidos en Leyes Especiales”. En: *Derecho Penal, Parte Especial*. Primera Edición. Tofulex, ediciones jurídicas. 2019. pp 709-713. Disponible en Vlex Chile

[37] Chile. Congreso Nacional. Artículo 366 y siguientes *Código Penal*. 1874.

[38] Chile. Congreso Nacional. Artículo 354 ter *Código Penal*. 1874.

Esta Ley agrega, en especial, recursos y herramientas para la investigación de los delitos antes descritos, como lo es entregar para su debido estudio y análisis los instrumentos informáticos o tecnológicos que las policías tienen permitido decomisar, como lo son los computadores, imágenes y sonidos, celulares, documentos, y en general todo otro tipo de elemento tecnológico que las policías incautaron, exigiendo entregarlos al Servicio Nacional de Menores, o en especial, a cualquiera de los organismos policiales especializados para la materia[39][40], como los son las ramas y brigadas especializadas de la policía de investigación.

Podemos ver que entonces se han hecho esfuerzos legislativos para expandir el tratamiento de los delitos que tienen por medio de comisión el internet, y que también se ha propagado respecto de los delitos de los que trata las modificaciones introducidas por la Ley 19.927, y se han ampliado las herramientas de investigación, atendiendo las formas y los medios por los cuales se utiliza y traslada el material objeto de este tipo de delitos, para facilitar y aumentar las herramientas de las fuerzas policiales.

2.3 Ley 21.459 de 2022 sobre Delitos Informáticos:

En función de los avances tecnológicos y la necesidad de actualizarse en este tema, y para adecuarse de mejor manera a convenios internacionales a los cuales Chile se encuentra suscrito, el año 2022 se promulga la nueva Ley 21.459 sobre delitos informáticos, que expande el catálogo de delitos de cuatro a ocho.

El contenido de esta Ley es bastante extensivo y reemplaza completamente a la Ley 19.223, quedando esta última derogada, y dando paso a una nueva Ley que comprende de mejor manera este tipo de delitos y actualiza sus contenidos y herramientas de investigación.

Como antes se dijo, la Ley contiene ocho delitos y un número de artículos accesorios a estos. El contenido de la Ley 21.459 será analizado fuera de orden para facilitar su comparación con los delitos contenidos en la Ley anterior:

a) El primer artículo de la Ley trata del delito de ataque a los sistemas informáticos, tipificando la acción de producir cualquier tipo de daño que afecte el funcionamiento del sistema en cuestión, incluyendo igualmente los datos que puedan encontrarse en dicho sistema informático. Este delito puede

[39] Chile. Congreso Nacional. Artículo 663 inciso 4° *Código Procesal Penal*. 2000.
[40] Chile. Congreso Nacional. Artículo 469 *Código Procesal Penal*. 2000.

ser homologable a la clasificación de sabotaje antes descrita, aunque esta nueva Ley actualiza el lenguaje y expande su alcance.[41]

b) El artículo cuarto no tipifica el ataque a los sistemas informáticos en sí, sino que directamente a los datos contenidos dentro de dichos sistemas informáticos que tengan como resultado la alteración, daño o supresión de estos. Este delito puede ser igualmente homologable a la clasificación de sabotaje informático antes vista.[42]

c) El artículo segundo de la Ley tipifica lo que se entiende como el acceso ilícito a un sistema informático sin autorización y superando las barreras propias de este tipo de sistemas, castigando más gravosamente la intención de apoderamiento de los datos contenidos dentro del sistema informático. Este delito puede entenderse dentro de la clasificación de espionaje informático antes revisada atendiendo a que dice relación con la forma en ilícita en que se obtienen datos pertenecientes a un sistema informático.[43]

d) El artículo tercero tiene como título la 'Interceptación ilícita', el cual dice relación con la afectación de la transmisión de datos informáticos no públicos hecha por un sistema informático o entre sistemas informáticos, al igual que la captación de dichos datos mediante sus emisiones electromagnéticas. El delito contenido en este artículo es igualmente homologable o comparable a la clasificación que se hizo respecto al espionaje informático.[44]

e) El artículo quinto presenta una figura delictiva nueva en el ordenamiento penal chileno, introduciendo la 'Falsificación Informática', que consiste en introducir, alterar, dañar o suprimir datos informáticos con el objetivo de que estos sean considerados como auténticos por un tercero, o sean utilizados para generar documentos auténticos, sin serlo. Se añade a la figura una agravante si quien realiza el acto es un empleado público. Esta es una figura nueva en la legislación sobre delitos informáticos, donde su versión

[41] Chile, Congreso Nacional. artículo 1 *Ley N° 21.459*. 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos
[42] Chile, Congreso Nacional. artículo 4 *Ley N° 21.459*. 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos
[43] Chile, Congreso Nacional. artículo 2 *Ley N° 21.459*. 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos
[44] Chile, Congreso Nacional. artículo 3 *Ley N° 21.459*. 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos

no informática se encuentra ya tipificada, siendo entonces que de esta forma se le da un tratamiento especial dada la condición del medio de comisión.[45]

f) El artículo sexto de la Ley introduce la figura de la receptación de datos informáticos, castigando la comercialización, transferencia y almacenamiento de cualquier dato informático obtenido por acceso ilícito, interceptación ilícita o falsificación de información, o que tengan otro fin ilícito. Tiene dos formas de comisión, y si se hace individualmente entonces su pena será más grave que si se comete con datos obtenidos como resultado de las conductas antes expuestas.[46]

g) El séptimo artículo de la nueva Ley sobre delitos informáticos trata el 'Fraude informático', esto es, causar perjuicio a otro con el objeto de obtener un beneficio de aquello, mediante la manipulación de sistemas informáticos, o la afectación, cualquiera sea el tipo de esta, de los datos pertenecientes a un sistema informático. Se castiga con distinta gradualidad dependiendo del valor del perjuicio causado.[47]

h) Por último, el artículo octavo introduce el concepto del 'Abuso de Dispositivos', que consiste en que, para realizar los hechos de los primeros cuatro artículos de la Ley 21.549, obtuviese o difundiese de cualquier forma programas informáticos, dispositivos, contraseñas o códigos, o cualquier dato de parecida naturaleza creados o modificados para la perpetración de dichos hechos.[48]

Estos son los delitos que agrega a nuestra legislación la Ley 21.549, que viene a reemplazar la anterior Ley sobre delitos informáticos, actualizando su contenido y lenguaje, y además contiene agravantes y atenuantes especiales para este tipo de delitos en específico.

I. Circunstancias Atenuantes: Se da como circunstancia especial que atenúa la gravedad de la pena la cooperación eficaz, entendiendo que

[45] Chile, Congreso Nacional. artículo 5 *Ley N° 21.459*. 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos
[46] Chile, Congreso Nacional. artículo 6 *Ley N° 21.459*. 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos
[47] Chile, Congreso Nacional. artículo 7 *Ley N° 21.459*. 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos
[48] Chile, Congreso Nacional. artículo 8 *Ley N° 21.459*. 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos

produce resultados en el esclarecimiento de los hechos investigados, o que sirve para prevenir o impedir que se perpetre cualquiera de los delitos antes descritos.

El artículo incluye qué se entiende por cooperación eficaz[49] y que deberá determinarse en la formalización de la investigación o en el escrito de acusación si la cooperación prestada por el acusado fue o no eficaz, reconociendo así la conducta del imputado como atenuante para la pena que se busca, tal como lo establece el artículo 9 inciso 2° de la Ley 21.459.

II. Circunstancias Agravantes: se presentan dos circunstancias agravantes especiales para este tipo de delitos[50]:

A. Que el delito informático sea cometido poseyendo una posición de confianza en la administración del sistema o de los datos informáticos, debido al cargo o posición ostentado respecto de dichos objetos.

B. Que el delito sea cometido aprovechándose el sujeto de la confianza o vulnerabilidad de menores de edad, adultos mayores o adolescentes. Podemos apreciar que se establece un mayor castigo en función de la búsqueda de mayor protección a sujetos entendidos como especialmente vulnerables al abuso o delitos cometidos a través de estos elementos tecnológicos.

Complementando los delitos anteriormente expuestos, la Ley 21.549 añade artículos específicos respecto a modificaciones o extensiones en cuanto a la investigación de los delitos contenidos en esta. A continuación, se explican los artículos relevantes para este trabajo de investigación.

1. Artículo 12: Este artículo se refiere a los primeros siete artículos de la Ley 21.549, que permite la utilización de las herramientas de investigación previstas en los artículos 222 al 226 del Código Procesal Penal, y que serán analizadas individualmente más adelante, con las siguientes especificaciones.

[49] Chile. Congreso Nacional. Artículo 9 inciso 2° *Ley 21.459* del 20 de junio de 2022.
[50] Chile. Congreso Nacional. Artículo 10 *Ley 21.459* del 20 de junio de 2022.

Al realizarse la orden que contenga alguna de las diligencias antes mencionadas, debe contener el nombre, alias y dirección física o electrónica del afectado por la medida en cuestión.

2. Artículo 12 inciso 3º: En este inciso se introduce la función del Agente Encubierto. Para su actuar, el Juez de Garantía puede ordenar, a petición del Ministerio Público, que uno o varios agentes policiales actúen bajo identidad incógnita, y así utilizar comunicaciones privadas con la finalidad de esclarecer los hechos objeto de la investigación, identificar a los perpetradores y comprobar los hechos.[51]

Para cumplir con sus funciones el agente encubierto tiene permitido enviar y recibir archivos que pueden considerarse ilícitos o contener material ilícito, por lo que, el agente encubierto se encuentra exento de responsabilidad criminal por todos los actos que deba realizar en relación con sus funciones, con ciertos requisitos, que sean necesarios para la investigación en desarrollo, y que guarden proporcionalidad con la finalidad de esta.

Por último, La Ley 21.549 contiene algunas disposiciones finales, en las cuales se incluyen las definiciones de los conceptos de mayor complejidad contenidos en la Ley[52], definiendo “Datos Informáticos”, “Sistema Informático” y “Prestadores de Servicio” en su artículo 16º, y así dando un mejor acercamiento al tratamiento de este complejo tema, que pueden servir para estandarizar los conceptos y tecnicismos más utilizados en el tema de los ciberdelitos. Estas definiciones, aunque útiles, son insuficientes frente a la gran cantidad de conceptos y temas que son abordados por el cibercrimen, para cuyas definiciones se requiere acudir a distinta legislación, y a la doctrina experta en los temas tecnológicos y que dicen relación al internet.

2.4 Código Penal y Código Procesal Penal:

El Código Penal contiene delitos que pueden formularse como ciberdelitos, para aquello solo se requiere que este tenga una modalidad digital o pueda tener como medio de comisión un sistema informático o el internet. Este trabajo se encargará de revisar todos aquellos delitos de los cuales la Brigada Investigadora de Ciberdelitos de la PDI se dedica a investigar, esto es, que se dedica de manera preferencial a investigar estos

[51] Chile, Congreso Nacional. artículo 12 *Ley N° 21.459*, del 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos
[52] Chile, Congreso Nacional. artículo 16 *Ley N° 21.459,* del 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos

delitos, ya que esta brigada participa de la investigación toda vez que elementos informáticos deban ser investigados, lo que incluye no sólo los delitos informáticos, sino que también los ciberdelitos en general, los cuales se encuentran contenidos en el Código Penal, entre estos podemos encontrar las estafas informáticas, delitos relacionados con menores de edad, entre otros.

El primer conjunto de estos delitos son las estafas informáticas o ciberestafas, compuestos principalmente por distintas formas de fraude que tienen como medio de comisión el internet.

Dos de estos delitos que destaca la Brigada investigadora de Ciberdelitos, como de especial cuidado, son los denominados “phishing” y “pharming”. El phishing es el acto mediante el cual los sujetos se hacen pasar por distintas personas o entidades financieras con el objeto de obtener los datos personales bancarios de las personas[53], esta es una modalidad de estafa de los artículo 248 del Código Penal que describe la estafa común[54], solo que de forma digital o en línea a través de internet, más comúnmente a través de correos electrónicos que aparentan ser direcciones de correo electrónico oficiales pertenecientes a casas comerciales, entidades bancarias, entidades oficiales del Estado, entre otras.

La segunda modalidad, el pharming, consiste básicamente en el mismo modo de operación, donde, comúnmente a través de correos electrónicos, un sujeto se hace pasar por una entidad oficial bancaria o financiera, del estado, o incluso como casas comerciales o entidades privadas de lotería ofreciendo cuantiosos premios, pero con la fundamental diferencia en que el objetivo no es la obtención de los datos personales ni de los datos bancarios, sino que el objetivo de plantar alguna forma de “malware”, o sea, de un programa dañino creado para extraer información, tomar computadoras o los datos contenidos en estas como rehenes, dañar directamente una computadora o los datos contenidos en ella, entre otras formas de alteración y daño que puede ser producido por este tipo de programas[55].

Otro conjunto de ciberdelitos investigados por esta Brigada de la Policía de Investigación son los delitos sexuales cometidos en contra de niños, niñas y adolescentes[56]. Este grupo de delitos se encuentra en el Código Penal y busca la

---

[53] OXMAN, Nicolás. “*Estafas informáticas a través de internet: Acerca de la imputación penal del “Phishing” y el “Pharming”*”. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso XLI. Chile. 2013. p. 215. Disponible en Vlex Chile

[54] Chile. Congreso Nacional. Artículo 248 *Código Penal*. 1874.

[55] OXMAN, Nicolás. Ob. Cit. 2013. p. 216. Disponible en Vlex Chile

[56] *Cibercrimen*, Policía de Investigaciones, 2020. Disponible en: Brigadas Investigadoras del Cibercrimen.

especial protección de este grupo vulnerable por estar más expuesto al internet, con modificaciones recientes al Código Penal para perseguir de mejor forma estos tipos penales.

En primer lugar, podemos encontrar los delitos relaciones a la producción, reproducción, almacenamiento y distribución de todo tipo de material pornográfico que haya sido producido con menores de edad participando en ellos, esto podemos encontrarlo en el artículo 366 del Código Penal en su primer inciso[57]. Acciones que pueden llegar a ser realizadas a través de internet, por lo que la Brigada de Investigación de Ciberdelitos de la PDI toma la tarea de investigar este tipo de delitos, donde menores de edad pueden ser explotados para la producción de material pornográfico a través de internet, al igual que ser distribuido y consumido por este mismo medio.

Otro tipo de ciberdelito sexual cometido en contra de menores de edad es el abuso sexual impropio del artículo 366 y siguientes del Código Penal, que describen las acciones abusivas, distintas del acceso carnal, contra menores de edad, como actos de significación sexual distintos de la violación, acceso carnal, incluso sin contacto físico con la víctima[58], por ejemplo, a través del internet. También, se castiga procurar la excitación sexual de menores y la actuación de conductas con significación sexual delante, en presencia o dirigidos a la víctima menor de edad[59]. Estos son los delitos sexuales contra menores de edad más comunes que son investigados por la Brigada Investigadora de Ciberdelitos de la PDI que se encuentran contenidos en el Código Penal.

Últimamente, autores como Claudio Cerda Santander, han destacado nuevos delitos de connotación sexual en contra de menores de edad, en específico se reconocen el “sexting” y el “grooming” o “childgrooming”, ambos son delitos relacionados a las redes sociales que han tenido relevancia últimamente por la participación de menores de edad en este tipo de aplicaciones y redes sociales[60].

Para combatir estas figuras se realizaron modificaciones al artículo 366 quáter del Código Penal a través de la Ley 20.526, modificando a la figura del nombrado ‘abuso sexual impropio’, buscando así proteger a los menores de edad de estas nuevas figuras delictuales. Cabe mencionar que el “grooming” no es técnicamente un delito, puesto que su figura no se encuentra precisamente tipificada en las normas citadas, sino que es una

---

[57] Chile. Congreso Nacional. Artículo 366 *Código Penal*. 1874.
[58] Chile. Congreso Nacional. Artículo 366 bis y 366 ter *Código Penal*. 1874.
[59] Chile. Congreso Nacional. Artículo 366 quáter incisos 2° y 3° *Código Penal*. 1874.
[60] CERDA SANTANDER, Claudio. “*Delitos informáticos crecen 74% en dos años y aumentan en casi todas las regiones*”. El Mercurio. Chile. 8 de abril de 2018. Recuperado de Delitos informáticos crecen 74% en dos años y aumentan en casi todas las regiones

modalidad criminológica[61], aunque se puede hacer una interpretación extensiva que permita entenderlo dentro de las figuras ya tipificadas por nuestra legislación.

El "grooming" proviene de la palabra y verbo en inglés "to groom" que significa acicalar o preparar, lo cual, conectada a las acciones sexuales que pueden cometerse contra niños, "grooming" o "childgrooming" se define como "*el proceso en donde un adulto desarrolla una relación de amistad con un niño, particularmente a través de internet, con la intención de tener con este una relación sexual ilegal*"[62]. Corresponde a una figura delictiva progresiva, donde el perpetrador busca progresivamente una relación con el menor afectado, ganando su confianza hasta cumplir con su objetivo de obtener material pornográfico del menor involucrado, mantener relaciones sexuales no físicas con este, o incluso llegar a obtener acceso físico al menor, como explica Christian Scheechler[63]. Los anteriores artículos del Código penal en relación al material pornográfico infantil, abuso sexual impropio, entre otros, fueron modificados para incluir y castigar las conductas que resultan del "grooming" como de esta conducta en general.

Por último, mencionar la figura, también reciente, del "sexting", relacionada a las conversaciones con connotación sexual entre adultos y menores de edad, que comúnmente se realizan a través de aplicaciones diseñadas para conversaciones, como también por redes sociales de distinto tipo, que puede llevar al intercambio de material sexual ilegal y de conductas sexuales ilegales entre adultos y menores, y no sólo a través de material escrito, sino que también a través de imágenes, video llamadas y otros medios a través de internet[64].

Las conductas descritas por el sexting, o al menos de las conductas en las que puede llegar a desarrollarse este tipo de actividades se encontraban cubiertas por el artículo 366 quinquies e incluso los del artículo 161, ambos del Código Penal[65].

Con esto se terminan de analizar las figuras delictivas relevantes para este trabajo de investigación, y será en base tanto a los delitos informáticos como a los ciberdelitos examinados que se estudiará la incidencia en cada etapa de la persecución penal de estos delitos por parte de los cuerpos policiales chilenos.

---

[61] SCHEECHLER CORONA, Christian. "*El childgrooming en la legislación penal chilena: sobre los cambios al artículo 366 quáter del código penal introducidos por la ley N° 20.526*". Revista Chilena de Derechos y Ciencia Política. Vol. 3, Nº 1. año 2012. p 61. Disponible en Vlex Chile

[62] Oxford Dictionaries [en línea]. *Grooming*. Definición 2. disponible en: grooming noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com

[63] SCHEECHLER CORONA. Ob .Cit. p 62. Disponible en Vlex Chile

[64] SCHEECHLER CORONA, Christian. "*Aspectos fenomenológicos y políticos-criminales del sexting. Aproximación a su tratamiento a la luz del Código Penal chileno*". Política Criminal. Vol. 14, Nº 27 de julio de 2019. p. 379. Disponible en Vlex Chile

[65] SCHEECHLER CORONA, Christian. Ob. Cit. p. 400. Disponible en Vlex Chile

2.5 De los Delitos Informáticos y Cibercrimen en la Actualidad:

Para comenzar con el análisis de lo que se entiende por delitos informáticos se debe precisar una definición que permita su aplicación al resto de este trabajo de investigación.

Antes que todo, debemos diferenciar entre los conceptos de Cibercrimen y Delito informático que, aunque apuntan a fenómenos y figuras ciertamente parecidas, no comparten una definición precisa que permita ahondar en su análisis. En primer lugar, Cibercrimen no posee una definición o significado preciso[66], pero para las funciones del presente trabajo de investigación bastará comprender al Cibercrimen como cualquier actividad delictiva que se desarrolle a través de un sistema informático, cualquiera sea su tipo, como un computador o dispositivo celular móvil, o de sus programas y funcionalidades, al igual que a través del acceso a internet[67]. Tomando como punto de partida este acercamiento al concepto del Cibercrimen, podemos entenderlo como la figura base, la cual puede manifestarse o materializarse entonces como un Delito informático, ya que este tiene como medio de comisión cualquier sistema informático, sus programas, y por supuesto las redes de internet. Pero podemos decir también que estos conceptos en realidad son homologables, y que apuntan al mismo significado.

En dicho sentido, Cibercrimen es un concepto amplio que nos sirve de umbral para cubrir una multiplicidad de figuras delictivas, incluso de delitos no tipificados como delitos informáticos u otros que se mencionan en este trabajo, delitos que pueden entenderse como comunes, que pueden llegar a tener una dimensión digital, informática, o que se relacionan a las redes de internet.

Cabe destacar la necesidad de dar mayor precisión a estos conceptos, debido a que, por la naturaleza del Cibercrimen y de este tipo de delitos, se requiere de una comprensión que abarque sus características y que nos otorgue un mejor entendimiento sobre cómo abordarlos desde el punto de vista de la investigación policial en el sistema penal.

Definiremos Delito Informático en la forma en que actualmente lo hace la nueva Ley de Delitos informáticos, la Ley 21.549, y también utilizaremos como definición la realizada por la ONU, que indica que el delito informático es “comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas

---

[66] CAVADA HERRERA, Juan Pablo. “*Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera”*. Asesoría Técnico Parlamentaria. Chile. julio de 2020. Disponible en: Asesoría Técnico parlamentaria

[67] CAVADA HERRERA, Juan Pablo. Ob. Cit. Disponible en: Asesoría Técnico parlamentaria

informáticos o los datos procesados por ellos"[68]. En la misma Ley mencionada anteriormente, el legislador expresa la intención de acercar el concepto de delito informático para mejor reflejar las exigencias que presenta el Convenio de Budapest sobre ciberdelincuencia[69].

Observamos entonces que existe una definición de delito informático, como delito que requiere únicamente de un medio, operaciones electrónicas, que entenderemos como el uso de cualquier sistema informático o sus programas, que atente contra la seguridad de los sistemas informáticos o sus datos. Una definición más completa nos la otorga la jurisprudencia, definiendo delito informático como "*todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática*"[70], lo cual veremos reflejado en cada uno de los delitos tanto de la Ley derogada acerca de delitos informáticos, como de la nueva Ley y de demás legislación que diga relación con delitos de esta naturaleza. En cuanto a la sana técnica informática, se puede entender que hace referencia al bien jurídico protegido por las normas sobre delitos informáticos, siento este "la calidad, pureza e idoneidad de la información en cuanto tal", como será revisado a continuación.

Bajo estas definiciones revisaremos a lo largo de este trabajo tanto los delitos informáticos, como ciertos aspectos del cibercrimen, por cuanto se encuentran relacionados en aspectos como la forma de investigación, debido a que comparten, por ejemplo, medios de comisión del delito y que ambos son investigados por una brigada especializada y profesionalizada de la Policía de Investigaciones.

Igualmente, se ha buscado definir cuál es el bien jurídico específico protegido a través de los delitos informáticos, aquello tiene una especial importancia para su interpretación y para la búsqueda de penas acordes al daño o situación de peligro que se realiza mediante un acto delictivo a dicho bien jurídico, por lo que definir en qué consiste es igual de importante para la investigación de estos.

---

[68] Naciones Unidas. "*Delitos Relacionados con las Redes Informáticas*". Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. Viena, Austria. 3 de febrero del año 2000. p. 5. Disponible en: Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente

[69] Consejo de Europa. "*Convenio sobre la ciberdelincuencia*". Budapest. 25 de octubre del año 2001. Disponible en: CONVENIO SOBRE LA CIBERDELINCUENCIA Budapest, 23.XI.2001

[70] Cuarta Sala de la Corte de Apelaciones de Concepción. Sentencia de la causa Resolución nº 9440 de la Causa nº 844 del año 2014. 30 de enero de 2015. Disponible en: Vlex Chile

La doctrina ha considerado dos posibles teorías para entender el bien jurídico protegido de los delitos informáticos[71]. En primer lugar, ver a los delitos informáticos como aquellos que tienen como bien jurídico protegido específico y único, el aspecto "informático" de estos, entendiéndose como la dimensión del medio de comisión delictiva, los sistemas informáticos y programas asociados. Y, en segundo lugar, una teoría que indicaría que los delitos informáticos no tienen un bien jurídico específico asociado a su medio de comisión o su característica "informática", sino que tienen un bien jurídico protegido general como los demás delitos.

El modelo que sigue la Ley 19.223 adopta la teoría que indica que los delitos informáticos tienen un bien jurídico específico y que no comparten un bien jurídico protegido general común con el resto de los delitos contenidos en el Código Penal, al reconocer de forma específica y a través de una Ley especial las figuras delictivas, que se describen como los Delitos Informáticos. Aunque podemos indicar que no solo tienen un bien jurídico protegido específico, sino que además persigue la protección de otros como veremos a continuación.

El bien jurídico protegido se expresó claramente en la Moción Parlamentaria de la Ley 19.223, donde se indica que este es *"la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan. Aquella, por el actual desarrollo tecnológico de la sociedad, merece ser protegida mediante la creación de figuras delictuales nuevas, que pongan de relieve su importancia"*[72], se expresa entonces un nuevo y único bien jurídico protegido para esta Ley y para este tipo de delitos en específico.

No obstante, no es correcto indicar que el único bien jurídico protegido es la calidad, pureza e idoneidad de la información y de su sistema informático asociado, puesto que los delitos informáticos son pluriofensivos, esto es, atentan contra más de un bien jurídico que protege la norma en concreto, como puede ser la privacidad o la identidad, ya que este tipo de delitos protege los datos contenidos dentro de los sistemas informáticos, los cuales comúnmente poseen información sensible relacionada a la identidad de las personas o tener contenido privado de estas, lo que significa que al sancionar conductas relacionadas a los datos contenidos en sistemas informáticos se protege un número amplio de bienes jurídicos, tanto los que se nombran en la ley, como

---

[71] MAYER LUX, Laura. "*El Bien Jurídico Protegido en los Delitos Informáticos*". Revista chilena de derecho vol. 44, no°1. Chile, Santiago. abril de 2017. Disponible en: EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS

[72] Chile, Congreso Nacional. *Moción Parlamentaria de Ley N° 19.223*, 16 de julio de 1991. Disponible en Historia de la Ley N° 19.223

igualmente la identidad y la privacidad de las personas a quienes dichos datos pertenecen y se buscan proteger a través de la ley.

En cuanto a la Ley 21.549, esta comparte el bien jurídico protegido mencionado para la Ley 19.223, esto podemos verlo reflejado en el mensaje de la Ley, que denota la necesidad de proteger especialmente a los medios informáticos, ello se observa en específico al mencionar las razones para dar especial protección en este ámbito:

"Las nuevas tecnologías desarrolladas en la economía digital permiten recolectar, tratar, almacenar y transmitir grandes cantidades de datos a través de sistemas informáticos, cambiando la forma de comunicarse entre las personas, así como también la manera en que se llevan a cabo diversas actividades laborales, comerciales y de servicios, incluidos aquellos de carácter o utilidad pública. Tal situación también ha implicado el surgimiento de nuevos riesgos y ataques contra bienes jurídicos social y penalmente relevantes, algunos de los cuales no se encuentran protegidos desde la óptica penal."[73]

De lo anterior podemos apreciar que se mantiene el bien jurídico protegido, modernizando su alcance para adecuarse al presente y prepararse para el futuro en cuanto a la tecnología. Siguiendo con dicha idea, la Ley 21.459 en su mensaje crítica y da fundamento para refundar las normas sobre delitos informáticos, indicando que:

"Desde el año 1993, Chile cuenta con la ley N° 19.223, que tipifica Figuras Penales Relativas a la Informática, legislación que no ha sido modificada desde su dictación, debiendo tenerse a la vista que, en la época de su entrada en vigencia, Internet era apenas un fenómeno incipiente y de escaso acceso a la ciudadanía. En el mismo sentido, las herramientas de persecución penal en esta materia datan del año 2000, fecha de dictación del Código Procesal Penal, que han devenido en insuficientes para una adecuada investigación en este tipo de ilícitos y con ello, resguardar los derechos de todos los intervinientes en el respectivo procedimiento."[74]

Por esta razón es de vital importancia comprender tanto la Ley 19.223, como la nueva Ley 21.459 en cuanto a los aspectos relacionados a la investigación de los delitos informáticos que componen a ambas, ya analizado en qué consiste el bien jurídico protegido de este tipo de delitos.

---

[73] Chile, Congreso Nacional. *Moción Parlamentaria de Ley N° 21.459*, 7 de noviembre de 2018. Disponible en: Historia de la Ley N° 21.459

[74] Ibídem.

A partir de lo anteriormente detallado respecto de los mensajes tanto de la Ley 19.223 como de la Ley 21.459 sobre delitos informáticos, podemos apreciar que se ha avanzado en cuanto a dilucidar en qué consisten los delitos informáticos y qué aspectos son especialmente relevantes de definir para facilitar los eventuales procedimientos de investigación. El mensaje de la Ley 21.459 reconoce que los avances tecnológicos han generado nuevas formas de delinquir en el espectro cibernético, por lo que se hizo necesario actualizar la legislación en dicho sentido y especialmente, expandir las herramientas disponibles a las policías para la adecuada investigación de este tipo de delitos.

Por último, la Ley 21.459 en su mensaje de igual forma reconoce la característica de pluriofensividad que poseen los delitos informáticos al decir que:

"*Finalmente, sobre la discusión en torno a la posibilidad de incluir estas materias en nuestro actual Código Penal, se ha estimado pertinente y en consideración de las características propias de estos tipos de delito, mantenerlo como una ley de carácter especial, en atención a los múltiples bienes jurídicos protegidos, no sólo la integridad o confiabilidad de la información contenidas en sistemas de información.*" [75]

En el último segmento del mensaje de la Ley, se aprecia que finalmente el bien jurídico protegido actualmente es "*la integridad o confiabilidad de la información contenidas en sistemas de información*"[76], además de los demás bienes jurídicos que merecen protección a través de estas normas, como la privacidad y la identidad de las personas.

Dicho esto, se consolida lo que son los delitos informáticos, pero se requiere realizar un análisis de sus disposiciones para apreciar los aspectos y características que llevan a que este tipo de delitos requiera de fórmulas y herramientas especiales para su investigación. Para esto, se requiere de un estudio respecto al contenido de las normas a revisar y las partes que las compongan, que ameritan la especial protección y las especiales herramientas de investigación.

Por último, en cuanto al concepto de Cibercrimen, este entendido como cualquier delito común contenido en el Código Penal que tenga como medio de comisión los sistemas informáticos o el internet, agregando además los delitos contenidos en leyes distintas que mantengan este carácter de cibercrimen, como puede ser los introducidos por la Ley 19.927, los cuales serán revisados únicamente por sus aspectos de

[75] Ibídem.
[76] Ibídem.

investigación, y que son llevados a cabo por la misma Brigada de la PDI que investiga los delitos informáticos.

2.5 Análisis formal de la Ley 19.223:

El contenido de esta Ley fue clasificado anteriormente, luego se analizaron las cuatro normas que describen los delitos o figuras delictivas que Chile tuvo hasta el año 2022, lo que representa la mayor parte de las investigaciones, casos, jurisprudencia y doctrina que fueron, y son, revisados para el presente trabajo de investigación, por lo que comprender los aspectos que hacen especiales a este tipo de delitos en concordancia con la norma que representa en su mayoría a la experiencia de nuestro país.

Como se dijo anteriormente, la Ley 19.223 solo consideraba cuatro figuras normativas en los cuatro artículos que la componían, sin mayor trabajo en expandir aspectos procedimentales o de investigación, por lo que no requiere de mayor extensión ni análisis, ya que basta con conocer su contenido y cómo esta fue utilizada para proteger los sistemas y datos informáticos.

Artículo 1º: "*El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectarán los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.*"

Lo primero que podemos indicar respecto de este artículo es que se configura un delito de resultado, esto significa que debe producirse como consecuencia de una acción, de la destrucción, es decir, dejar inutilizable un sistema informático, impedir, obstaculizar o modificar su funcionamiento, esto se agrega a la mera acción que produce estos resultados e indica que no es suficiente para determinar el delito, sino que se requiere en definitiva que estos resultados se produzcan, así lo explica Aníbal Manríquez[77], y es la forma en que se entienden este tipo de delitos. De esto último se desprende igualmente, que también se tipifica cualquier acción que tenga como resultado la afectación del correcto funcionamiento de un sistema informático y sus componentes, generando la destrucción o inutilización de estos.

En la segunda parte de este artículo, se agrega a la tipificación la afectación de los datos contenidos dentro del sistema informático por consecuencia de cualquiera de

[77] CORNEJO MANRÍQUEZ, Aníbal. "*Derecho Penal. Parte General y Especial en preguntas y respuestas*". 5° edición. Corman Editores Jurídicos. Año 2021. p. 80. Disponible en: Vlex Chile

las conductas descritas en su primera parte. Se aprecia que los resultados de daño e impedimento de funcionamiento pueden caer sobre cualquier parte del sistema informático, como lo son sus componentes o la totalidad de la maquinaria computacional, pero cabe agregar que estos sistemas pueden ser elementos que no son computadoras en específico, como celulares, elementos de almacenamiento de datos como tarjetas de almacenamiento o discos de almacenamiento, los cuales pueden ser objeto de lo expresado en el artículo.

Cabe agregar respecto de este artículo que requiere de una intencionalidad maliciosa al indicar "*el que maliciosamente*", esto agrega un carácter subjetivo al delito, requiriendo no solo probar el resultado, sino que igualmente deberá probarse la intencionalidad del autor para lograr una condena.

Con esto podemos inferir que para una eficiente y eficaz investigación de los aspectos objetivos y subjetivos de este delito, que arrojen insumos probatorios suficientes para alcanzar el estándar probatorio necesario para un sentencia condenatoria, se requiere de acceso tanto al sistema informático en sí, como de sus componentes físicos y de sus aspectos digitales relacionados a los datos contenidos en estos, para lo cual se requiere de un nivel de experticia y profesionalización en quienes tienen la labor de levantar insumos probatorios en la investigación.

Por último, cabe agregar que este delito puede considerarse dentro de la clasificación doctrinaria de Sabotaje Informático[78], del cual forman parte dos de los delitos contenidos en esta Ley.

Artículo 2º: "*El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.*"

En primer lugar, y para todos los delitos informáticos, se requiere para la comisión de este la existencia de un sistema informático que pueda ser objeto de los delitos tipificados, que si bien puede parecer evidente, es posible requerirse que se sujete o no a prueba este hecho para continuar con la acción penal[79].

En la dimensión objetiva del delito descrito podemos ver que, en primer lugar, la acción corresponde a usar o conocer la información contenida en un sistema informático

[78] CHÁVEZ CHÁVEZ, Eric Andrés. "Décimo Grupo: Delitos Contenidos en Leyes Especiales". En: *Derecho Penal, Parte Especial*. Primera Edición. Tofulex, ediciones jurídicas. 2019. pp 709-713. Disponible en: Vlex Chile

[79] Primera Sala de la Corte de Apelaciones de Copiapó. Resolución nº 15 de la Causa nº 448 de 2018. 19 de diciembre de 2018. Disponible en: Vlex Chile

de manera indebida, ante lo cual podemos sostener que “indebidamente” significa tener conocimiento o usar la información sin ser el dueño y no teniendo autorización para conocerla o utilizarla. En una segunda parte se añade al delito interceptar, interferir la información o acceder al sistema informático; suponemos que a estos verbos rectores se incluye la necesidad de que sean efectuados de manera indebida.

El artículo no describe las formas en que una persona puede llegar a apoderarse, usar, o conocer de la información contenida en un sistema informático, al igual que no menciona las formas en que puede ser interceptada o interferida; esto da una posibilidad de adaptación acorde con los avances tecnológicos sin que ello afecte la persecución de la figura tipificada, debido a que pueden considerarse todas las nuevas formas y medios para cometer este delito que surjan y que ya surgieron con los avances de la tecnología durante todo el tiempo en que esta Ley se mantuvo vigente.

Respecto de la dimensión subjetiva de este delito, el artículo requiere del ánimo de apoderarse, usar o conocer indebidamente la información contenida en el sistema informático, por lo que debe probarse que quien efectúe los actos de interceptar, interferir o acceder a dicha información lo hizo con el ánimo de apoderarse de la información para sí mismo, utilizarla, o simplemente conocerla, de manera indebida.

Por último, en cuanto a este artículo, podemos clasificar la figura descrita como “Espionaje Informático”[80], en cuanto esta dice relación con la obtención de acceso a la información contenida en el sistema, sin describir más allá de utilizar la palabra “indebidamente”, siendo los verbos rectores del delito interceptar, interferir o acceder, aunque parte de la jurisprudencia ha considerado este delito como parte de lo entendido como “Sabotaje Informático”[81].

Artículo 3º: “*El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.*”

En el aspecto objetivo del delito analizado, la conducta prescrita es la de alterar, dañar o destruir de cualquier forma los datos contenidos en un sistema que maneje dichos datos informáticos o información, por lo tanto, este es otro delito que puede considerarse como uno de resultado que se introdujo con la Ley. Destrucción de los datos significa que estos no puedan ser recuperados; mientras que alteración o daño apuntarán

[80] CHÁVEZ CHÁVEZ, Eric Andrés. “Décimo Grupo: Delitos Contenidos en Leyes Especiales”. En: *Derecho Penal, Parte Especial*. Primera Edición. Tofulex, ediciones jurídicas. 2019. pp 709-713. Disponible en: Vlex Chile

[81] Primera Sala de la Corte de Apelaciones de Copiapó. Resolución nº 15 de la Causa nº 448 de 2018. 19 de diciembre de 2018. Disponible en: Vlex Chile

al impedimento del buen funcionamiento o del funcionamiento programado para los datos del sistema informático, por lo que pueden ser dos los resultados que requiere la conducta tipificada. Más específicamente la jurisprudencia ha definido "Alterar los datos contenidos en un sistema" como "*ingreso o introducción de datos erróneos, el borrado de datos verdaderos, transformaciones o desfiguraciones de los datos, y en general toda conducta que implique cambiar la información contenida en un sistema de tratamiento de la misma sin destruirla*"[82], en general, son todas las acciones que modifican la información del sistema, al igual que las que las destruyen y dañan los datos.

En la dimensión subjetiva, el delito requiere que las acciones antes descritas se realicen maliciosamente, buscando el resultado dañoso, por lo que no cabe describir como delito casos accidentales o cuando se produzca el resultado sin desearlo o sin querer causar cualquier tipo de daño. Esto se traduce en que las acciones que sin buscar que se dañen o destruyan los contenidos del sistema informático producen dicho resultado no son castigadas, siempre y cuando se logre probar la inexistencia de la intención maliciosa. Por supuesto, el daño o destrucción del elemento físico que contiene los datos también puede significar la destrucción de los datos, por lo que este delito es extensivo a acciones que salen del enfoque meramente informático y que deben ser considerados en su investigación.

Cabe agregar que este delito se entiende dentro de la clasificación de "Sabotaje informático" antes utilizada, ya que dice relación con lo que se realiza o cómo se afecta al sistema informático en cuestión, y no en la obtención de los datos contenidos en este o de la obtención de acceso a éste.

Este delito es el equivalente al descrito en el artículo primero de esta misma Ley, solo que en vez de sabotaje del sistema informático en sí y sus componentes, este artículo y delito dice relación respecto de los datos que se encuentran en este.

Artículo 4°: *"El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."*

En primer lugar, revisando la parte objetiva del delito, los verbos rectores que dirigen la acción tipificada son los de revelar o difundir los datos contenidos en un sistema informático, esto significa que se requiere que estos datos fuesen privados y no

[82] Cuarta Sala de la Corte de Apelaciones de Concepción. Considerando 5º de la Resolución nº 9440. Causa nº 844 de 2014. 30 de enero de 2015. Disponible en: Vlex Chile

accesibles fácilmente. Segundo, que estos deben estar contenidos en el sistema de información, aquello puede ser una computadora o un servidor que contenga datos, igualmente, como se mencionó anteriormente, puede referirse a los elementos de almacenamiento de datos que han permitido los avances tecnológicos.

En cuanto al sujeto activo nos encontramos con una particularidad en la tipificación del delito en cuestión, ya que se castiga con mayor gravedad a la persona que realiza la acción siendo el responsable del sistema informático, esto significa que si quien siendo el encargado del sistema y que, por tanto, es quien tiene como obligación el resguardo de la integridad y privacidad de los datos contenidos en el sistema informático, realiza el tipo penal, será castigado con más gravedad, por lo que, para configurar el aumento de castigo al tipo penal, se requiere que el sujeto que realice la acción posea la cualidad de ser el responsable o encargado del sistema que contiene los datos que fueron finalmente revelados o difundidos maliciosamente.

Respecto a su dimensión subjetiva, se requiere que las acciones antes descritas sean realizadas con una intención maliciosa, de querer realizar la acción y además de causar daño o afectar de quien sus datos están siendo revelados o difundidos a través del delito, por lo que es otro aspecto que debe ser demostrado.

Este delito presenta un especial desafío en términos de investigación, debido a que la revelación y difusión de cualquier tipo de datos digitales en la actualidad puede efectuarse de diversas formas y utilizando medios tanto físicos como digitales en los cuales la información puede ser revelada y difundida, desde redes sociales y correos electrónicos, hasta las redes de internet en general, donde puede representar una alta dificultad rastrear tanto el origen de la información, como la identidad de quienes la difunden. Además de dificultarse la investigación toda vez que, al momento que la información y datos se vuelven públicos, determinar quién los reveló por primera vez puede significar una tarea incluso más ardua en términos de investigación, ya que este delito perfectamente puede llevar a la comisión de otros, como pueden ser las injurias y calumnias utilizando datos extraídos, entre otros tipos de delitos, si se incurre en cualquier tipo de error o no se logra dar con quien es la persona que comienza con la difusión.

Por último, en cuanto a este artículo, cabe agregar que pertenece a la clasificación de “Espionaje Informático”, ya que dice relación con la intención maliciosa de

los datos contenidos en un sistema informático y su posterior difusión, cualquiera sea la forma o medio[83].

[83] CHÁVEZ CHÁVEZ, Eric Andrés. “Décimo Grupo: Delitos Contenidos en Leyes Especiales”. En: *Derecho Penal, Parte Especial*. Primera Edición. Tofulex, ediciones jurídicas. 2019. pp 709-713. Disponible en: Vlex Chile

Capítulo 3: La actual Ley 21.459

A continuación, se efectuará una síntesis de los delitos informáticos en la actualidad analizando la Ley que fue promulgada el año 2022, explicando sus especificaciones y realizando las comparaciones pertinentes con la ley que viene a derogar.

3.1 Análisis Formal de la Ley 21.459:

La Ley 21.459 fue introducida el año 2022 para actualizar las conductas tipificadas como delitos informáticos, adecuándolas de mejor forma a la modernidad y preparándolas para los avances tecnológicos. Además, tuvo como objetivo cumplir lo dispuesto en el Convenio de Budapest, convenio ratificado por Chile que tiene como tema principal la ciberdelincuencia, y mandata a los países firmantes a tipificar una multiplicidad de conductas como delitos.

En cuanto a su contenido, duplica la cantidad de delitos informáticos que poseía Chile, además de expandir diferentes ámbitos, como lo es el procedimiento y en especial la investigación de este tipo de delitos. En este acápite, se analizará cada uno de los delitos tipificados para determinar las características especiales que presentan, analizar sus requerimientos de mayor especialización y las nuevas herramientas otorgadas para su investigación.

Artículo 1º: "*Ataque a la integridad de un sistema informático. El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en sus grados medio a máximo.*"[84]

Los verbos rectores de este delito son obstaculizar e impedir, y el objeto es el funcionamiento total o parcial del sistema informático, por tanto, no se requiere de un resultado específico, sino que solo el acto de impedir de cualquier forma el funcionamiento normal del sistema es castigado. A continuación, el artículo expresa las formas en las que se puede obstaculizar o impedir el funcionamiento del sistema en cuestión, esto es, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos contenidos en el sistema informático, esto significa que no se

[84] Chile, Congreso Nacional. artículo 1° *Ley N° 21.459*, 20 de junio de 2022.

castiga la afectación de la dimensión física del objeto que contiene el sistema informático o sus partes, sino que únicamente se sanciona la afectación de sus datos por alguna de las formas descritas, ya sea eliminándolos del sistema, cambiándolos o alterándolos de forma que sean inutilizables o no fueran útiles para su objetivo.

Este artículo mantiene el contenido del artículo 3º de la Ley 19.223, agregando que la afectación no solo puede ser total, sino que puede ser parcial; además, incluye distintas formas en las que pueden verse finalmente afectos los datos contenidos en el sistema, pero principalmente, establece que lo que se castiga no es esta afectación, sino que el impedimento y alteración del correcto funcionamiento del sistema y de sus datos, no así la destrucción o alteración de estos últimos.

A diferencia de su versión del artículo 3º de la Ley 19.223, el delito presentado en esta Ley no requiere de una intencionalidad "maliciosa" para ser castigado, se prescinde de aquella, formulándose entonces un delito que puede entenderse como un delito de resultado, donde lo que se requiere para la configuración del hecho punible es que, en primer lugar, se produzca el resultado de obstaculización o impedimento del correcto funcionamiento del sistema informático, para entender esto se utilizará la definición común de obstaculizar[85], esto significa que no pueda ser utilizado para sus funciones comunes o específicas, siendo este el resultado que configura el delito; y en segundo lugar, se desprende una lista no taxativa, donde se requiere de un medio o forma para la producción de los resultados. Por lo tanto, se elimina dicha parte de la dimensión subjetiva de este delito.

Al observar los resultados requeridos, al igual que la multiplicidad de modos en los que puede darse la comisión del delito, se concluye que puede darse en muchas formas dependiendo de las capacidades tecnológicas que existen para dañar, deteriorar o destruir datos informáticos, tanto desde el acceso que se puede obtener a un sistema informático, como para lograrlo de manera remota a través de internet o programas especialmente creados para causar este tipo de daños tanto al sistema informático en sí, como a los datos contenidos en este.

Artículo 2º: "*Acceso ilícito. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.*

[85] Real Academia Española [en línea]. Disponible en obstaculizar | Definición | Diccionario de la lengua española | RAE - ASALE

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo."[86]

El segundo artículo de la Ley 21.459 describe el delito de acceso ilícito, esto es, superando la autorización que se posee en cuanto al acceso a cualquier sistema informático, superando las barreras tecnológicas de seguridad utilizadas para evitar el acceso a sujetos no deseados o a quienes en efecto no poseen la autorización necesaria, o simplemente ignorando la autorización, accedan al sistema informático. Por tanto, nos vemos nuevamente frente a un delito de resultado, donde se describen distintas formas en que puede llegar a cometerse el mismo acto de acceder al sistema informático sin autorización o excediendo la autorización que sea posea, cabe mencionar que a quienes se dedican a dicha actividad se les conoce como "cracker"[87], aunque dicha definición no dice relación con su intención, sea inocua o maliciosa.

En primer lugar, podemos apreciar que existe una marcada diferencia con el artículo 2º de la Ley 19.223, en cuanto dicha norma únicamente consideraba como sujetos a quienes acceden al sistema habiendo sido personas externas a este, es decir, personas que no tenían acceso permitido y que actúan sin efectuar un acto ilícito hasta que se cumple con los demás requisitos para la comisión del delito, aunque existe doctrina y jurisprudencia que ha considerado que, en función de los bienes jurídicos protegidos por la Ley 19.223, se podría considerar como sujeto en dicho artículo tanto personas externas como internas al sistema informático[88].

Es importante la mención a las barreras técnicas y medidas de seguridad, estas son una parte importante de los sistemas informáticos que no fueron mencionadas en la anterior ley vigente. Estas barreras pueden verse presentadas en distintas formas y métodos de protección acorde a los sistemas informáticos, y comprender sus tipos y funcionamientos es un hábito indispensable para su investigación, por lo que la experticia en la protección de datos y de sistemas informáticos es integral para la correcta

---

[86] Chile, Congreso Nacional. artículo 1° *Ley N° 21.459*, 20 de junio de 2022.

[87] Diccionario Panhispánico del español jurídico. disponible en: Definición de cracker - Diccionario panhispánico del español jurídico - RAE

[88] WINTER ETCHEBERRY, Jaime. "*Elementos típicos del artículo 2° de la Ley Nº 19.223: Comentario a la SCS de 03.07.2013 Rol Nº 9238-12*". Revista Chilena de Derecho y Ciencias Penales. Vol. II, Nº 4. p. 279. Disponible en: delito del artículo 2º de la ley nº 19.223 esPionaJe inforMático. bienes JurÍdicos Protegidos. aPoderaMiento, uso y conociM

especialización de los agentes que llevarán a cabo la investigación. En su segundo inciso, se añade la posibilidad de que se obtuviese acceso con un objetivo en específico, esto es, apoderarse de la información contenida en el sistema informático, lo que se analizará en lo que se entiende por dimensión subjetiva del delito.

A continuación, se añade a la tipificación la conducta de divulgar la información a la cual se accede, abriendo la posibilidad a todo tipo de formas en las que se puede difundir la información, como lo son las redes sociales, o en general las redes de internet.

En cuanto a la dimensión subjetiva, no es hasta el segundo inciso en que se dispone que se castigará más gravemente cuando las acciones descritas en el primer inciso sean realizadas con la intención de apoderarse de la información que se encuentra contenida en el sistema informático al que se accede; además de esto, no encontramos nada fuera de lo común, sin requerir una intencionalidad más allá de la mera intención de cometer u obtener el resultado al que hace referencia el delito.

Por último, en su primer inciso, este artículo se aprecia como una evolución del segundo artículo de la Ley 19.223, en el cual, era punible el acceso a los contenidos de un sistema informático, es decir, la interceptación y acceso a los datos, sin tener una forma de castigar el mero acceso al sistema en sí, por lo que la conducta tipificada requería tanto del acceso a los datos, como además, de una intención de hacer dichos datos suyos, o difundirlos de alguna forma, sin tener forma de sanción el acceso al sistema que las contiene; esto se suple en el segundo inciso del artículo presente, puesto que se castiga el ánimo de apoderarse de la información o datos contenidos en el sistema informático al que se obtiene acceso, al igual que penar la divulgación y difusión de la información, sancionando más gravemente el caso en que sea la misma persona quien obtiene y difunde la información.

Esta intencionalidad de difundir los datos que son obtenidos mediante las conductas tipificadas es una evolución del artículo 4º de la Ley 19.223 que describe dicha conducta. Actualmente no se requiere de una intención maliciosa y se describen de mejor forma los medios en los que puede ser configurada la conducta.

Este delito presenta especiales dificultades para su debida investigación, entre estos se encuentran los relacionados al acceso al sistema informático en sí o el acceso a una computadora, como también el aspecto de las autorizaciones para investigar y cómo se obtienen estas. Por supuesto, se debe incluir la faz subjetiva incluida en el segundo inciso, en cuanto a la intención de apoderamiento de los datos, un aspecto que podría

llegar a presentar dificultades al momento de la producción de insumos probatorios y en la investigación.

Artículo 3º: "*Interceptación ilícita. El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.*

El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo."[89]

El artículo tercero describe el delito de "Interceptación Ilícita", plasmado de forma comparable al delito que se encontraba contenido en el artículo 2º de la Ley 19.223, puesto que utilizan algunos de los mismos verbos rectores como "Interceptar".

A diferencia de la ley anterior, la Ley 21.459 extiende las conductas que pueden ser entendidas como "interceptación ilícita"; estas son, el que indebidamente intercepte, interrumpa o interfiera la transmisión no pública de información contenida en un sistema informático o de una comunicación entre dos o más de ellos, por tanto, en este nuevo tipo penal, interceptar puede significar distintas actividades, como obtener acceso a la información que transmite un sistema informático, o también lograr acceso a llamadas y mensajes realizados entre computadores o celulares, es concretamente el acceso indebido a información, sin que se requiera el acceso al sistema informático que la contiene.

A lo anterior, se añaden otros dos verbos o acciones catalogados como interceptación ilícita, estos son la interrupción y la interferencia. La interrupción se refiere a impedir la transmisión de información por parte de un sistema informático, o imposibilitar la comunicación de información entre dos de estos sistemas que buscan transmitir datos entre ellos.

Por último, la interferencia puede significar la interrupción no permanente, o la alteración de cualquier tipo de los datos transmitidos por un sistema informático, que se condice con las definiciones expresadas por Eric Chávez[90].

---

[89] Chile, Congreso Nacional. artículo 3° *Ley N° 21.459*, 20 de junio de 2022.

[90] CHÁVEZ CHÁVEZ, Eric Andrés. "Décimo Grupo: Delitos Contenidos en Leyes Especiales". En: *Derecho Penal, Parte Especial*. Primera Edición. Tofulex, ediciones jurídicas. 2019. pp 709-713. Disponible en: Vlex Chile

Además, a esta faz objetiva del delito se añade que todas estas conductas deben realizarse a través de medios técnicos, esto es, utilizar como medios de comisión, elementos tecnológicos que sirvan para la comisión del delito, lo que incluye todas las técnicas, tecnologías, programas, entre otros, que sirvan para la interceptación de datos informáticos. Pero estos elementos evolucionan y se vuelven cada día más sofisticados y efectivos, por lo que, exige que los agentes policiales tengan conocimiento y comprensión técnica y profesional respecto para el efectivo combate de este tipo de delitos.

El segundo inciso de este artículo añade a las conductas tipificadas en su inciso anterior, la captación de información ya no a través de medios técnicos, sino que, por medio de la captación de las emisiones electromagnéticas producidas por la transmisión de la información por un sistema informático, esta descripción es altamente extensiva, por lo que se añade que para configurarse el delito no se debe contar con la autorización necesaria para su captación. A su vez, para la captación se requiere de instrumentos especializados para este acto, con lo cual se puede captar las ondas provenientes de todo tipo de elementos utilizados para la transmisión de información contenida en sistemas informáticos, ya sean antenas o dispositivos más sofisticados.

En cuanto a la faz subjetiva del delito no se aprecian mayores complejidades que las que deben ser consideradas para todo tipo de delitos, ya que no se establecen requisitos relativos a la intención del sujeto activo.

Este delito contiene una mayor abundancia técnica que los anteriores, esto presenta una mayor dificultad para su investigación debido a que la especialización de los sujetos y herramientas, y la profesionalización requerida para la investigación de elementos como la interceptación de datos transmitidos por sistemas informáticos es alta, la identificación de los sujetos activos en el delito, los métodos para discernir quienes participan en las conductas tipificadas, entre otros, dificultan las labores de persecución del delito y deben ser estudiadas las capacidades de nuestras policías para la superación de estas.

Artículo 4º: "*Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.*"[91]

[91] Chile, Congreso Nacional. artículo 4° *Ley N° 21.459*, 20 de junio de 2022.

El artículo 4º tiene como título “Ataque a la integridad de los datos informáticos”, y posee en su faz objetiva como verbos rectores, alterar, dañar o suprimir, en este caso, datos informáticos. Suprimir claramente indica la destrucción permanente, o aparentemente permanente, de los datos, cualquiera sea la forma en que se hagan desaparecer dichos datos. También se utilizan los verbos alterar y dañar, ante los cuales se requiere hacer una distinción puesto que, aunque dañar incluye una alteración en sí misma de los datos, esta implica una alteración que altere las funciones comunes del dato en cuestión o de su correcto funcionamiento, creando una incapacidad para su correcto uso o lectura, mientras que alterar no implica una pérdida de funcionamiento o capacidad de lectura de los datos informáticos.

Los verbos incluidos tienen una condición agregada, esto es, que tanto alterar, como dañar y suprimir sean realizados indebidamente, de forma que no se tenga autorización o permiso para realizar cualquiera de las acciones antes descritas, por lo que, para que la acción sea calificada como delito de Ataque a la integridad de los datos, se requiere que dichas acciones sean realizadas de manera indebida.

El delito presenta un último requisito en su tipificación, éste es que se cause un daño grave al titular o dueño de los datos, pero la presente ley no describe lo que se entiende por daño grave por el cual pueden ser afectados el titular. Este daño grave, en el caso de los delitos informáticos se ha entendido como la destrucción o total inutilización del elemento en cuestión, y que sea esta destrucción o inutilización lo que provoca este grave daño a la víctima del delito[92].

En cuanto a la faz subjetiva no encontramos indicaciones más allá de las comunes para todos los delitos.

Cabe agregar que, este artículo tiene su propia versión en la anterior Ley 19.223, realizando distintos avances en su tipificación. En primer lugar, se elimina parte de la faz subjetiva, puesto que el artículo anterior requería de una intencionalidad maliciosa, cosa que no forma parte del delito en esta Ley y, en segundo lugar, se reemplazó con la calidad de “indebida” requerida para las acciones tipificadas, al igual que requerir de un resultado de daños al titular, lo cual no se encontraba en el delito en la Ley anterior.

Por último, se deben mencionar las características que posee el delito, que pueden requerir de herramientas o procedimientos especiales para su investigación. Si bien la alteración, daño o supresión de datos informáticos son fenómenos que no

[92] ÁLVAREZ FORTTE, Héctor. “*Los Delitos Informáticos*”. Revista Jurídica Regional y Subregional Andina. Edición 9°. Chile. Año 2009. p. 111. Disponible en: Vlex Chile

presentan mayores dificultades que las herramientas para detectar la alteración de los datos informáticos, si puede haber dificultad para determinar el daño producido por el delito en el titular o dueño de los datos informáticos afectados.

Artículo 5º: "*Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo.*

Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo."[93]

El delito de falsificación informática es una innovación legislativa en comparación a la ley anterior, al no corresponderse con la definición y contenido de ninguno de los cuatro delitos informáticos contenidos en la anterior Ley 19.223.

Con respecto a la faz objetiva del delito, volvemos a encontrarnos con el requerimiento para la conducta tipificada, de que se realice indebidamente. Los verbos rectores presentes en el delito son introducir, alterar, dañar o suprimir datos informáticos y, a primera vista, parecería repetir el contenido del artículo cuarto, únicamente agregando la exigencia de introducción de datos, esto significa agregar datos nuevos a un sistema que antes no los poseía.

Aunque parece ser el mismo artículo anterior agregando un conducta tipificada, no es hasta que analizamos la faz subjetiva que nos encontramos con el nuevo delito, se requiere para la comisión del delito la intención de que los documentos introducidos o afectados tengan por objetivo ser considerados como auténticos cuando no lo son o para producir nuevos documentos con esta apariencia de autenticidad o documentos que de hecho sean auténticos, pero que tengan como documentos que se utilizan para su producción documentos falsos o falsificados, por lo que todas las acciones tipificadas requieren ser realizadas con la intención descrita.

El segundo inciso añade una tipificación especial cuando el sujeto que cometa el delito sea empleado público, siempre y cuando realice los actos abusando de su oficio o posición.

Este delito presenta la particularidad de que requiere la utilización de estos para alcanzar los resultados de alterar, suprimir o introducir datos a un sistema informático

[93] Chile, Congreso Nacional. artículo 5° *Ley N° 21.459*, 20 de junio de 2022.

para hacerlos pasar como documentos oficiales o auténticos cuando no lo son o para generar nuevos documentos para hacerlos pasar como auténticos, esto presenta particularidades a la investigación puesto que, debe determinarse la intención de crear o utilizar estos datos como documentos auténticos, y si estos llegan a ser utilizados para dicha intención, se debe determinar la autenticidad de los documentos y la autenticidad en su origen, lo cual puede presentar dificultades en la investigación; aunque perfectamente se pueden concluir que puede no existir manera de utilizar estos documentos falsificados sin conocerlo, pero estas son particularidades de la investigación que no necesariamente competen a la labor de los agentes policiales.

Este delito presenta una especialidad, puesto que hace referencia al concepto de documentos, lo cual puede ser especialmente amplio debido a que en el campo de la informática dicho concepto es comúnmente utilizado para referirse a un conjunto de archivos y contenido de carácter informático, pero es en el sentido jurídico de estos que debe ser aclarado para la correcta aplicación del artículo[94].

La ampliación del concepto de documento es ampliado a entender también a los documentos electrónicos, definiéndose estos en la ley 19.799: "*toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior*"[95], por lo que puede entenderse la alteración y utilización de este tipo de documentos como el objeto de esta norma, de igual forma que se entiende para la anterior Ley 19.223, para lo cual, se requiere de una interpretación extensiva de lo que se entiende por destrucción y alteración de datos informáticos, bajo el sabotaje informático, tal y como explican Jaime Vera y Laura Mayer[96], en esta oportunidad de forma más específica con un nombre específico para este acto, denominado entonces falsificación electrónica.

Artículo 6º: "*Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado.*"[97]

---

[94] CANELO, Carola; ARRIETA, Raúl; MOYA, Rodrigo y ROMO, Rodrigo. "*El Documento Electrónico. Aspectos Procesales*". Revista Chilena de Derecho Informático. N°4, mayo de 2004 pp. 81-106. Disponible en: Revista Chilena de Derecho Informático

[95] Chile, Congreso Nacional. artículo 2° *Ley N° 19.799*, 10 de octubre de 2014.

[96] MAYER LUX, Laura; Vera Vega, Jaime "*El documento como objeto material de las falsedades documentales y del sabotaje informático en el Derecho penal chileno*". Polít. crim. Vol. 14, Nº 27, julio 2019. Art. 12, pp. 440-441. Disponible en: http://politcrim.com/wp-content/uploads/2019/05/Vol14N27A12.pdf

[97] Chile, Congreso Nacional. artículo 6° *Ley N° 21.459*, 20 de junio de 2022.

Este artículo introduce una nueva figura delictual denominada “Receptación de datos informáticos”. En su faz objetiva apreciamos que el sujeto que, conociendo del origen o pudiendo conocer del origen de los datos informáticos en cuestión, comercialice, transfiera o almacene los datos con los fines ilícitos que revisaremos a continuación, será castigado con la pena que establece el artículo presente; esto significa que primero se requiere, para tipificar una conducta bajo este delito, que el sujeto conozca del origen o que pudiera conocerlo. El origen del que habla la Ley corresponde a que los datos informáticos en cuestión hayan provenido de las conductas descritas en los artículos 2º, 3º y 5º de la misma Ley, esto es, a través del Acceso Ilícito, la Interceptación Ilícita y de la falsificación informática, por lo que se requiere que el sujeto que realiza la conducta descrita en este delito sepa que los datos que utilizará para este se hayan obtenido de manera ilícita.

En cuanto a los verbos rectores del delito estos son comerciar, transferir y almacenar. El primero de estos corresponde a la compra y venta de los datos informáticos para cualquier uso y por cualquier medio para lo cual se requiere entonces de una transacción monetaria, la RAE define comerciar como “*dedicarse a la compraventa o el intercambio de bienes o servicios*”[98], por lo que se entiende que la compra y venta de los datos informáticos objeto de este delito. El segundo es la transferencia, transferir de una persona a otra los datos informáticos a través de cualquier medio, por lo que no se requiere que medie un pago o intercambio para que ocurra el delito. Por último, tenemos el almacenamiento de dichos datos obtenidos de manera ilícita, por supuesto la transferencia requiere del almacenamiento de los datos y la comercialización requiere tanto del almacenamiento como de la transferencia de estos, por lo que la tipificación del delito cubre desde el punto mínimo de lo que puede realizarse con los datos informáticos hasta su posible transferencia y comercialización.

En cuanto a la faz subjetiva del delito se requiere tanto del conocimiento del origen ilícito de los datos informáticos objeto de las conductas tipificadas y su posterior utilización con el objeto de continuar con las acciones ilícitas de los artículos 2º, 3º y 5º de la Ley, por lo que se requiere determinar la intención de acción ilícita del sujeto, agregando que puede corresponderse a cualquiera de los artículos antes mencionados, como de cualquier otra conducta ilícita.

Como se puede apreciar del artículo, para su investigación se requiere, además de comprobar las conductas tipificadas, que como mínimo requieren de un elemento de

[98] Real Academia Española [en línea]. Definición 1. Disponible en comerciar | Definición | Diccionario de la lengua española | RAE - ASALE

almacenamiento y que pueden requerir de un comprador o persona o sistema al que los datos serán transferidos, que los datos en cuestión fueren obtenidos por los delitos descritos en artículos anteriores, por lo que se requiere comprobar tanto un delito anterior a la receptación de datos informáticos que sirva como medio de obtención de los datos receptados, como los elementos propios de la receptación que requieren de elementos probatorios.

Por último, agrega la situación de quien sin haber cometido los actos de los delitos de los artículo 2º, 3º y 5º, sepa que los datos que trata fueron conseguir mediante estos o debiera saberlo, es igualmente castigado, requiriendo probar el conocimiento de la comisión de los delitos que sirven como medio, como también de la capacidad de conocimiento de dicha situación, lo cual puede significar un a dificultad, toda vez que es difícil comprobar estas situaciones cuando los datos tienen un origen ilícito del cual no se tiene conocimiento público o de serlo es difícil el acceso es esto.

Artículo 7º: "*Fraude informático. El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado:*

1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales.

2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.

3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales.

Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.

Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito."[99]

Este delito es el más extenso de esta ley y corresponde al "Fraude informático", el cual presenta especiales particularidades y su extensión legislativa merece de un estudio más extensivo, puesto que corresponde a una variante del delito de fraude, definido en el sentido de *"causar un perjuicio de carácter pecuniario en los intereses del Estado, lo que puede suceder –como señala la disposición– empleando engaño o consintiendo en que se defraude, lo que involucra que el empleado abuse de la confianza depositada en él, y no cumpla con sus funciones*"[100], cuando este sea cometido a través de un medio informático como lo son las redes de internet.

Presenta gradaciones de la pena asociada al delito dependiendo de la cuantía o valor calculable al perjuicio producto del delito, al igual que particularidades en su faz subjetiva y en cuanto al sujeto del delito.

En primer lugar, respecto del sujeto del delito, en su primer inciso se refiere a "el que", por tanto, se refiere al sujeto que realiza las acciones o conductas que se describen en el resto del artículo, presentando una particularidad en el inciso final, donde se castiga con autoría del delito a quien también no solo realiza las conductas descritas sino a quien conociendo o pudiendo conocer de estas, las facilita los medios para su comisión al autor.

Respecto a la faz objetiva del delito, cabe agregar los verbos utilizados para describir la acción tipificada, el cual es manipular un sistema informático; esto significa provocar una alteración, cualquiera sea, a un sistema informático que produzca un cambio en su funcionamiento, en sus datos, o en el funcionamiento de estos últimos. A continuación, el artículo describe los medios en los que puede manipularse el sistema, mediante la introducción, alteración o supresión de los datos contenidos en este, de modo que utiliza conceptos que fueron revisados anteriormente. La diferencia se presenta en que el delito del Fraude Informático requiere de un resultado, que la acción cause finalmente un perjuicio a otro, que este sea cuantificable, y dependiendo de la cuantía calculada a los perjuicios se castiga de manera respectiva.

En cuanto a la faz subjetiva, las conductas tipificadas tienen como verbos rectores manipular un sistema informático, con ciertos medios o formas específicas; estas son,

[99] Chile, Congreso Nacional. artículo 1° *Ley N° 21.459*, 20 de junio de 2022.
[100] GARRIDO MONTT, Mario. "*Derecho Penal. Parte General. Tomo III*". Chile: Editorial Jurídica de Chile, 2010. p 455. Disponible en: Vlex Chile

alteración, daño o supresión de datos pertenecientes a un sistema informático a través de cualquier medio técnico.

Este delito, por ser una versión "informática" de un delito ya existente como es el fraude, presenta ciertas particularidades, de modo que se pueden asimilar métodos de investigación y de las herramientas disponibles para el Ministerio Público y para las policías.

Para la imputación, en primer lugar, se requiere probar tanto la acción de manipulación de los datos del sistema informático o de los datos contenidos en este, como también el medio en que se manipulo dicho sistema; en segundo lugar, se requerirá probar la intención de obtener un beneficio monetario por el sujeto que realiza las acciones tipificadas en el delito; y, por último, probar la concurrencia de los perjuicios y de su monto. Se debe agregar la situación especial del último inciso del artículo, en cuanto a probar el conocimiento o la capacidad de conocer, al igual que concurrir en la acción de facilitar los medios para la comisión del delito.

Sin embargo, no es correcto hacer una mera asimilación de las conductas entre el fraude informático y su versión no informática, dado que el fraude informático se ha comprendido con un conjunto de conductas que van más allá de la sola perpetración de un fraude haciendo uso de medios tecnológicos o informáticos para su comisión, sino que ha comprendido conductas o delitos como el "phishing" y "pharming"[101] que se estudiarán más adelante en esta investigación, sin considerar que estos dos últimos delitos también han sido y pueden ser considerados como ciberdelitos y no necesariamente caben dentro de la clasificación de delitos informáticos.

Artículo 8º: "*Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales.*"[102]

El último de los delitos introducidos por la Ley 21.459 se denomina "Abuso de los Dispositivos", y tiene por objeto tipificar la utilización y otras acciones que se pueden

[101] MAYER LUX, Laura. "*Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos*". Revista Lux et Praxis. Nº 1. Año 2018. Chile. p. 174. Disponible en: Vlex Chile
[102] Chile, Congreso Nacional. artículo 8° *Ley N° 21.459*, 20 de junio de 2022.

realizar respecto de dispositivos, datos, programas, códigos de acceso o seguridad, entre otros, que fueron creados o modificados de cualquier forma para perpetrar delitos específicos, los del artículo 1º a 4º de la Ley 21.459, o sea el ataque a la integridad de un sistema informático, el acceso ilícito, interceptación ilícita y ataque a la integridad de los datos, agregando las conductas contenidas en el artículo 7º de la Ley 20.009, esto es el delito de "uso fraudulento de tarjetas de pago y transacciones electrónicas", el cual posee una lista taxativa de conductas tipificadas como también herramientas y medidas propias para su correcta investigación.[103]

En cuanto a la faz objetiva del delito, el sujeto activo será quien, con el objeto de perpetrar los delitos nombrados anteriormente, realice la conducta tipificada. Para esta los verbos rectores son entregar, obtener, importar, difundir o cualquier forma que permita poner a disposición, programas computacionales, contraseñas, códigos de seguridad y cualquier dato similar que fuesen creados para la perpetración. De los verbos rectores se desprende que se castiga tanto la puesta en disposición de elementos diseñados o modificados para la perpetración de ciertos delitos, como también de la obtención de estos, cualquiera sea el medio de obtención o disposición.

Respecto de la faz subjetiva del delito, se requiere que la intención del perpetrador sea la de haber realizado los actos tipificados para la perpetración de los delitos nombrados, por lo que el tipo penal no exige que se perpetren dichos delitos incluyendo que existiese la intención de perpetrarlos, o sea, que el objetivo de poner a disposición u obtener el elemento que sirve como medio para la perpetración, se haya hecho con dicha intención; por lo tanto, corresponde a un delito de peligro concreto, el mero hecho de que se entreguen u obtengan los elementos que se utilizarían o son creados específicamente para la comisión de los delitos descritos es suficiente para que se entienda el delito por concretado[104].

El abuso de dispositivos requiere de elementos especializados para cometer delitos específicos, por lo que en la investigación del delito se requiere que dicho elemento exista y cumpla con las características de haber sido creado o modificado para ese específico propósito, y por supuesto, requiere que este elemento fuese obtenido o puesto a disposición por el sujeto imputado; estas dos acciones son muy distintas y castiga dos caras del mismo acto, sancionando a quien obtiene el elemento y quien lo comercializa o entrega. A esto debemos agregar la intención con la que deben efectuarse

---

[103] Chile. Congreso Nacional. Ley N° 20.009 de 18 de marzo de 2005. Disponible en: Ley 20.009

[104] MATUS ACUÑA, Jean Pierre; POLITOFF LIFSCHITZ, Sergio y RAMÍREZ G, María Cecilia. "*Lecciones de Derecho Penal chileno. Parte Especial*". s.n. Chile. Editorial Jurídica de las Américas. 2009. p 157. Disponible en: Vlex Chile

los actos, la intención de cometer los delitos nombrados en el artículo, algo que debe probarse para la imputación.

3.2 De los demás artículos de la Ley

Los demás artículos contenidos en la Ley 21.459 hacen referencia a aspectos procesales, y otros aspectos que dicen relación con las normas anteriores y, en concreto, con los delitos informáticos.

Algunos de estos artículos serán revisados y analizados en este trabajo bajo la investigación realizada por los agentes policiales, por el momento no serán revisados y se dejan para más adelante en este mismo trabajo, por su importancia respecto de la participación de agentes policiales en dicho ámbito.

Capítulo 4: De la investigación de los delitos informáticos y cibercrimen por parte de la PDI:

Como se mencionó en los capítulos anteriores, son las policías en su labor de apoyo y ayuda al Ministerio Público las que, a través de sus facultades y órdenes del Fiscal a cargo de la investigación, llevarán a cabo todas las actividades, diligencias y actuaciones necesarias para levantar los insumos probatorios que se utilizarán en un eventual juicio oral para determinar la culpabilidad o inocencia de un imputado por un delito informático.

Como también se determinó anteriormente, la policía que se encargará por excelencia de todas las diligencias investigativas es la Policía de Investigaciones, haciendo uso de todas sus facultades y herramientas. La PDI a su vez hará uso de su brigada especializada para dicho cometido, la Brigada de Investigación del Cibercrimen, la cual lleva a cabo las tareas investigativas para este tipo de delitos, contando con herramientas especializadas e individuos especial y profesionalmente preparados para aquello, contando con todas las facultades entregadas por el Código Procesal Penal y por las leyes específicas que tocan los temas pertinentes a esta brigada y la investigación especial de estos.

El último capítulo de la presente investigación tiene por objetivo determinar y analizar el rol de Carabineros y Policía de Investigación en la investigación y levantamiento de insumos probatorios frente al cibercrimen y en específico en los casos de delitos informáticos, considerando la pertinencia, efectividad y posibilidad de mejora en la especialización y herramientas aplicadas para esta tarea en específico, analizando entonces el alcance de las facultades de las policías y su incidencia en la investigación y persecución del cibercrimen.

4.1 La Brigada Investigadora del Cibercrimen

Para cumplir con las funciones de investigación y protección de la ciudadanía, la PDI posee un número importante de brigadas y unidades especializadas en distintas áreas, contando tanto con laboratorios de criminalística especializados por tipos delictuales, como con centros o brigadas de personal especializado para los diferentes tipos de delitos investigados[105], es dentro de este contexto donde encontramos la Brigada investigadora del Cibercrimen, la cual tiene el deber de investigar los delitos informáticos

[105] *Unidades Especializadas*, Policía de Investigaciones, Disponible en: Unidades Especializadas

y del cibercrimen en general, es decir, los fenómenos delictuales objeto de esta investigación.

Debido a los crecientes avances tecnológicos han emergido nuevas figuras delictivas relacionadas con los sistemas informáticos y por supuesto con el internet, para esto, la Brigada Investigadora del Cibercrimen cuenta con las herramientas y la especialización necesaria para combatir, principalmente, los delitos informáticos[106]. Así, la brigada se concentra principalmente tanto en los delitos de Sabotaje, lo que se entendería compuesto por los artículos 1º y 4º de la Ley 21.459, la cual utiliza vocabulario y denominaciones distintas para describir los delitos que se entienden por Sabotaje informático, y Espionaje informático, descrito por los artículos 2º y 3º de la misma ley sobre delitos informáticos, como también en los ciberdelitos asociados a la "explotación sexual de menores a través de internet"[107].

Además, la brigada ha sido dispuesta para la investigación de delitos no informáticos y que no corresponden al cibercrimen, toda vez que es pertinente la investigación de elementos que tengan relación con el internet y las telecomunicaciones, en investigación, por ejemplo, de delitos de injurias y calumnias donde parte de estos sean realizados a través de internet o redes sociales y su propagación.[108]

La página web sobre cibercrimen que pertenece a la PDI, además de describir lo dicho en el párrafo anterior, entrega consejos a la ciudadanía para mantener la ciberseguridad de sus computadoras, sus datos, y de los menores de edad, dando consejos e instrucciones de cómo navegar el internet de forma segura y cómo mantenerse alerta a posibles fraudes y conductas que puedan vulnerar datos o a menores de edad[109].

Esta brigada cuenta desde noviembre del año 2022 con un nuevo Cuartel General de Cibercrimen[110] que busca alojar en un mismo lugar a todas las unidades de la PDI que tengan relación con la investigación de delitos que tienen como vía de comisión el internet y que tengan como objeto del delito sistemas informáticos y la vulneración de derechos sexuales de niños, niñas y adolescentes.

---

[106] *Cibercrimen*, Policía de Investigaciones, 2020. Disponible en: Brigadas Investigadoras del Cibercrimen.
[107] *Cibercrimen*, Policía de Investigaciones. Ob. Cit.
[108] Segunda Sala de la Corte Suprema. Resolución nº 8042-2009. 25 de enero de 2010. Disponible en: Vlex Chile
[109] Cibercrimen, Policía de Investigaciones. Ob. Cit.
[110] MARITANO, Ana. "*Chile – Inauguran Cuartel Nacional de Cibercrimen*". Diario Jurídico [en línea]. Chile. 1 de noviembre de 2022. Disponible en: Chile – Inauguran Cuartel Nacional de Cibercrimen - Diario Jurídico

La tarea realizada por esta brigada ha tomado especial relevancia durante los últimos años, debido al alza en tendencias de comisión de delitos informáticos como el fraude informático, sabotaje informático y de figuras relacionadas al abuso sexual a través de internet. Según datos de la PDI, entre 2017 y 2021 los anteriores delitos que figuraban en la Ley 19.223 como sabotaje y espionaje informático, han aumentado en un 95% y en un 61% respectivamente, en el mismo periodo de tiempo[111], para datos actualizados respecto de los nuevos delitos descritos por la Ley 21.459 se debe esperar a que nuevas investigaciones, datos y sentencias se desprendan de dicha legislación y sean contabilizadas por la PDI. Sin embargo, tenemos información sobre las formas en que la Brigada ha participado en la investigación de delitos informáticos, como al utilizar especiales técnicas para recuperar datos que se creían borrados o eliminados de una computadora y para levantar los insumos probatorios necesarios para probar la culpabilidad o inocencia del imputado, importancia señalada por autores como Alberto Contreras[112].

Cuenta este cuartel, y por tanto, la Brigada de investigación de Cibercrimen de la PDI, con un equipo especializado de investigación de delitos informáticos, un equipo de investigación contra el abuso sexual de niños, niñas y adolescentes a través de internet y con un departamento forense digital[113], los cuales en conjunto investigan todas las figuras delictivas estudiadas en este trabajo.

Entonces, se entiende a la Brigada de Investigación de Cibercrimen de la PDI como el principal actor a la hora de investigar los delitos informáticos y los ciberdelitos en general, con niveles de especialización adecuados para esta tarea y con herramientas, equipos y departamentos especializados que conforman un conjunto de agentes policiales que se encargan de la investigación de estos delitos.

4.2 De las herramientas generales de investigación

Las herramientas con las que cuenta el Fiscal a cargo de la investigación para dicha labor se encuentran contenidas en el Código Procesal Penal, al igual que en las leyes para delitos especiales que contengan herramientas o procedimientos especializados para los delitos que tratan.

---

[111] Policía de Investigaciones. "*Nuevo Complejo Policial contra el Cibercrimen*". Chile. 27 de octubre de 2022. Disponible en: Nuevo Complejo Policial contra el Cibercrimen

[112] CONTRERAS CLUNES, Alberto. "*Delitos Informáticos: un importante precedente*". Revista Ius et Praxis. V.9 n.1. Chile, Talca. Año 2003. p. 4. Disponible en: Ius et Praxis II. JURISPRUDENCIA DELITOS INFORMÁTICOS: UN IMPORTANTE PRECEDENTE

[113] CONTRERAS CLUNES, Alberto. Ob. Cit., p 5-7.

Dentro del procedimiento ordinario aplicable al cibercrimen en general y a los delitos informáticos, tanto en el caso de la anterior Ley 19.223 y la Ley 21.459, encontramos las "actuaciones de investigación" en los artículos 180 y siguientes del Código Procesal Penal, describiendo distintas herramientas y diligencias utilizadas en la etapa de investigación del procedimiento ordinario.

El Código Procesal Penal permite al fiscal practicar "*todas aquellas diligencias pertinentes y útiles al esclarecimiento y averiguación del mismo* (el delito), *de las circunstancias relevantes para la aplicación de la ley penal…*"[114], teniendo como única limitación que se utilice alguno de los medios previstos en la Ley, esto es, que las herramientas utilizadas se encuentren descritas en el Código Procesal Penal o en una de las leyes especiales.

Una de las diligencias más importantes que pueden ser consideradas a la hora de realizar la investigación, es la posibilidad de incautación de los objetos, documentos e instrumentos que fueron utilizados o parecen haber sido utilizados para la comisión del hecho que reviste la apariencia de delito, o también estos mismos objetos cuando sirvan como prueba y hayan sido hallados en el lugar de comisión del delito[115]. Esto presenta un desafío en cuanto a los delitos informáticos, debido a que si bien se puede determinar cuáles son los objetos, sistemas y dispositivos que fueron utilizados para la comisión de un delito, se requiere de la incautación del artículo 216 del Código Procesal Penal para su obtención.

Estos artículos presentan una especialidad y es la posibilidad de incautar elementos cuando estos se encuentren en el "lugar del suceso", pero en los delitos informáticos y en los ciberdelitos o cibercrimen en general, no encontramos un lugar físico de suceso. En estos casos no hablamos de un sitio del suceso en el mero sentido físico del lugar especial en el que se hace uso de los dispositivos y sistemas informáticos para la comisión del delito, sino que también de los espacios virtuales o digitales mediante los cuales se pueden obtener y levantar insumos probatorios[116], como puede ser una página de internet que puede contener datos e información relevantes para la investigación, o también las redes sociales donde pueden levantarse evidencias, y los servidores que mantienen y guardan la información sujeta a ser investigada, por lo que se requiere de una ampliación del concepto de sitio del suceso para que así se dé una eficaz investigación.

---

[114] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 180, inciso 2°. 2000

[115] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 187. 2000

[116] BATARCE, Catalina. "*El sitio del suceso para la policía ya no es sólo físico, también es virtual*". La Tercera [en línea]. Chile. 29 de julio de 2022. Disponible en: El sitio del suceso para la policía ya no es sólo físico, también es virtual - La Tercera

Para la obtención de acceso físico a los dispositivos utilizados para la comisión del delito, o sea todas las herramientas físicas como discos de almacenamiento, celulares, computadores, y por supuesto todos los elementos físicos que pueden contener evidencias de la comisión de los delitos, se debe aplicar lo establecido en el artículo 205 del Código Procesal Penal que permite la entrada y el registro del lugar donde se puede encontrar el imputado y los elementos y medios utilizados por este, aquello requerirá o no de una autorización judicial dependiendo de la diligencia en específico a practicar.

Otra de las diligencias de vital importancia para la producción de insumos probatorios es la incautación de objetos y documentos, lo cual según establece el artículo 217 del Código Procesal Penal, permite a las policías incautar los objetos y documentos que puedan servir como medios de prueba dentro del procedimiento, lo cual permitiría lograr acceso a los documentos no solo físicos sino que también digitales si se realiza una interpretación amplia de qué significa documento[117]; por supuesto, esto no es estrictamente necesario siempre que bajo objetos podemos comprender todos los elementos que contengan los datos informáticos y documentos digitales que puedan servir para los mismos propósitos que los descritos anteriormente.

El mundo digital mantiene algunas de las comunicaciones como la telefonía y la correspondencia, aunque esta última sea digital o electrónica. El artículo 218 del Código Procesal Penal permite la incautación de comunicaciones como la correspondencia, indicando que “la retención de la correspondencia postal, telegráfica o de cualquier otra clase”[118]; esto nos da a entender que la correspondencia electrónica o digital se encuentra cubierta por este artículo que permite la incautación y retención de estos elementos no físicos, para dejar aún más claro que se hace uso de una definición extensiva de correspondencia es que se agregó en su primer inciso que pueda obtenerse copias y respaldos de la correspondencia electrónica que pueda servir para la investigación que haya sido enviada o recibida por el imputado.

4.3 De las diligencias relacionadas a las comunicaciones

A continuación, se revisarán las diligencias que dicen relación con la capacidad para interceptar, almacenar y utilizar las comunicaciones del imputado como medio de prueba relevante para la investigación, todo esto se encuentra contenido en el Código Procesal Penal.

---

[117] Chile. Congreso Nacional. Artículo 217 *Código Procesal Penal*. 2000.
[118] Chile. Congreso Nacional. Artículo 218 *Código Procesal Penal*. 2000.

En primer lugar, debemos revisar el artículo 222 sobre la interceptación de comunicaciones telefónicas[119], que permite a las policías interceptar todo tipo de comunicaciones que reciba o transmita el imputado a través de dispositivos digitales o informáticos, ya sea por llamadas telefónicas, mensajes de texto, y otros tipos de comunicaciones que veremos a continuación.

La interceptación de comunicaciones telefónicas nos permite acceder a todo tipo de comunicaciones realizadas por un teléfono cuando se sospeche de la comisión de un delito, o que una persona planea en algún momento cometer un delito, siempre y cuando la investigación hiciera imprescindible la utilización de este medio de investigación para aquella, puesto que este tipo de diligencias investigativas afectan directamente la privacidad no solo del imputado, sino que también de las personas con las que mantiene comunicaciones las cuales serán interceptadas[120]. No todas las comunicaciones pueden ser interceptadas, se encuentra prohibida la interceptación de las comunicaciones entre el imputado y su abogado mientras no se tenga una orden judicial debidamente fundada por el tribunal[121].

Para interceptar las comunicaciones referidas en este capítulo se obtendrá el apoyo de las compañías telefónicas y de internet para obtener el acceso a las líneas del imputado, para ello, las compañías referidas deben mantener un registro de las comunicaciones y de las direcciones IP de las personas involucradas en dichas comunicaciones. En cualquier momento si las sospechas de comisión de delito que hacen posible la interceptación de comunicaciones desaparecen por cualquier motivo entonces la diligencia debe cesar inmediatamente por parte de la policía que realiza la diligencia[122].

Los métodos y herramientas a las que tiene alcance las policías para interceptar y almacenar comunicaciones telefónicas se revisarán más adelante en esta investigación, luego de analizar los métodos utilizados por la brigada especializada de la PDI para esta tarea.

Todas estas diligencias deben ser debidamente informadas al imputado y a quienes afecte esta investigación, al igual que seguir todas aquellas reglas del Código Procesal Penal respecto a las diligencias de investigación[123].

---

[119] Chile. Congreso Nacional. Artículo 222 *Código Procesal Penal*. 2000.
[120] ALVARADO URÍZAR, Agustina. "*El Control de la Resolución Motivada que Autoriza una Interceptación Telefónica en Chile y Duración de la Medida*". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso. XLIII. Chile. Año 2014. Disponible en: Vlex Chile
[121] Chile. Congreso Nacional. Artículo 222 inciso 3° *Código Procesal Penal*. 2000.
[122] Chile. Congreso Nacional. Artículo 222 inciso 5° *Código Procesal Penal*. 2000.
[123] Chile. Congreso Nacional. Artículo 224 *Código Procesal Penal*. 2000.

4.4 De las Diligencias especiales a los Delitos Informáticos

La Ley 21.459 sobre delitos informáticos sólo incluye una diligencia investigativa de especial aplicación para la investigación en casos de delitos informáticos, esta es la figura del "agente encubierto", una figura que en su variante digital o "en línea" es nueva para el ordenamiento jurídico chileno.

En los delitos y crímenes no cibernéticos o informáticos "*(...) son agentes encubiertos aquellos funcionarios policiales que actúan en la clandestinidad, generalmente con otra identidad, y que desempeñan tareas de represión y prevención del crimen mediante la infiltración en organizaciones criminales a fin de descubrir a las personas que las dirigen, recabando pruebas y prestando testimonio de cargo ante la justicia*"[124]. Los agentes encubiertos son funcionarios pertenecientes a la policía de investigaciones que se adentran en los grupos delictuales, a través de identidades distintas a la real, con el objetivo de pasar desapercibidos dentro de estas y así recabar información relevante para la investigación de los delitos, por supuesto, en su variante informática el agente encubierto cumple la misma función, solo que aprovechando de anonimato que permite el internet, se adentra e introduce en grupos, foros, páginas y todo tipo de comunidades de internet de modo anónimo con el fin de obtener información sobre actividades delictivas actuales, pasadas y futuras, evitarlas o eventualmente llevarlas a los tribunales.

El agente encubierto que deberá, o no, participar en las actividades de estos grupos delictivos, puede únicamente obtener comunicación con estos grupos para obtener información, como también puede hacerse parte de estos y para aquello la normativa lleva consigo aparejada la protección y defensa del agente policial en caso de ser necesaria la participación de este en los delitos previstos por la Ley. Esto a través de la garantía por participación en hechos delictivos en función de su labor como agentes encubiertos.

Esta herramienta ha sido ampliamente utilizada para la investigación de otros delitos, pero es una figura reciente para el caso de los delitos informáticos, añadida a la legislación chilena en la Ley 21.459 del año 2022. En el caso de los delitos informáticos es la única herramienta especialmente diseñada e introducida en la legislación para su aplicación en casos de delitos informáticos, aunque perfectamente es utilizable para la investigación del cibercrimen en general y para todo tipo de ciberdelitos.

---

[124] RIQUELME PORTILLA, Eduardo. "*El agente encubierto en la ley de drogas. La lucha contra la droga en la sociedad del riesgo*". Política Criminal. s.n. Chile. s.f. Disponible en: Vlex Chile

Podemos indicar entonces, que el agente encubierto dentro del contexto de los delitos informáticos es aquel funcionario policial que utilizando el anonimato, se introduce en las comunidades y redes por internet con el fin de averiguar la identidad de los sujetos involucrados en actividades delictivas, la ocurrencia de dichas actividades y buscar recopilar y levantar insumos probatorios para dichos fines, para lo cual deberá entablar relaciones con los sujetos involucrados, utilizando una falsa identidad diseñada y preparada para obtener la confianza de los sujetos y ser parte de sus actividades y contactos.

Para poder realizar las actividades de agente encubierto se requiere de autorización judicial, tal como lo establece el artículo 9 del Código Procesal Penal[125], debido a la infracción o afectación del derecho de privacidad de los sujetos involucrados al realizarse las diligencias en servidores, canales, foros o redes privadas de internet, las cuales no se encuentren a disposición pública.

La identidad falsa o ficticia no requiere de una identidad real aparejada, esto es, de nombre, apellidos, R.U.T, u otros elementos de identificación personal, ya que, por la naturaleza del internet, estos no son necesarios debido a que es común la utilización de nombres de usuario ajenos a la identidad real de quien utiliza dicho nombre, utilizados en redes sociales, foros, etc., para ocultar la identidad y mantener el anonimato que es característico del medio, carácter peligroso y que ha significado especial preocupación, tal y como lo explica Margarita Robles al referirse al anonimato en los ciberespacios[126].

Para mayor exactitud, el agente encubierto no digital encuentra su definición en la Ley 20.000, en su artículo 25, alrededor de la investigación de delitos de tráfico de estupefacientes[127], con tres objetivos específicos que son aplicables a la definición del agente encubierto informático:

- Identificar a los participantes de actividades delictivas o grupos organizados para delinquir.
- Reunir información acerca de estos individuos, grupos y sus actividades.
- Recoger todos los antecedentes necesarios para la investigación de los delitos y actividades en cuestión.

---

[125] Chile. Congreso Nacional. Artículo 9 *Código Procesal Penal*. 2000.
[126] ROBLES CARILLO, Margarita. "*El ciberespacio: presupuestos para su ordenación jurídico - internacional*". Revista Chilena de Derecho y Ciencia Política. Vol. 7 N° 1. Chile. 22 de enero de 2016. p. 21. Disponible en Vlex Chile
[127] Chile. Congreso Nacional. Artículo 25 *Ley N° 20.000* de 16 de febrero de 2005.

Siguiendo la definición que se utilizó anteriormente, estas son también las finalidades del agente encubierto en su versión digital.

La utilización de esta herramienta digital no será exclusiva de los delitos informáticos, es posible su utilización en otros ciberdelitos, como lo puede ser el delito de posesión e intercambio de pornografía infantil, a través del artículo 369 del Código Penal[128] que termina refiriéndose igualmente a la nombrada Ley 20.000 que contiene la definición de agente encubierto.

En la investigación del cibercrimen utilizan el agente encubierto para los fines fijados por la Ley, igualmente se realiza mención especial de esta figura para los delitos informáticos y su investigación en específico, debido a la utilidad y versatilidad de la herramienta a través de las redes de internet. A continuación, se revisarán un número de diligencias y herramientas utilizadas para investigar el cibercrimen en general, que son aplicables igualmente a los delitos informáticos por su naturaleza digital.

4.5 Diligencias Digitales y herramientas para la investigación del Cibercrimen

Carabineros y la policía de investigación utilizan herramientas y diligencias para determinar la identidad de personas sospechosas de delito, como elementos biológicos, huellas dactilares, entre otras herramientas para identificar elementos no biológicos como balas, drogas, etc.[129] Pero no son aplicables estas herramientas a la dimensión digital, se requiere, como se dijo anteriormente, de herramientas especializadas que ayuden a las policías a investigar en el plano informático.

Las evidencias se desprenden de los rastros o elementos que son fuente de estas y que pueden ser los mismos datos contenidos en un sistema informático en forma de documentos, claves o contraseñas, “cookies”, datos de identificación, imágenes, archivos de audio y video, mensajería instantánea, mensajería vía correo electrónico, contenidas en toda forma de medios, computadoras, elementos de almacenamiento, chips de identificación, entre muchos otros.

Estas evidencias pueden ser obtenidas de manera digital, interviniendo con los objetos que retienen los datos relevantes para la investigación que pueden servir de evidencia para esta, obteniéndola a través de pericias, como las realizadas por el agente encubierto o, por supuesto, a través de la obtención física de los medios que contienen

[128] Chile. Congreso Nacional. Artículo 369 *Código Penal*. 1874.
[129] CORNEJO MANRÍQUEZ, Aníbal. “*Medicina legal, criminalística y criminología. Preguntas y respuestas*”. 3a edición. Chile. Corman Editores Jurídicos. 2022. Disponible en: Vlex Chile

estos, requisando los diferentes tipos de elementos que pueden contener la información, documentos y datos, para a través de las pericias y conocimientos necesarios en informática, extraer toda esta información para ser procesada y analizada en busca de evidencias.

Es por lo anterior, que podemos separar la investigación a realizar entre la dimensión física y la digital. La primera dice relación con la obtención de los medios que contendrán los elementos sujetos a la segunda dimensión, ya que los elementos digitales se encuentran contenidos, o solo se puede obtener acceso a estos, mediante la dimensión física de la investigación.

Un ejemplo altamente utilizado es el de los correos electrónicos, si estos son interceptados o descubiertos en un sistema informático como una computadora o teléfono celular, se debe analizar no solo el contenido del correo electrónico en cuestión, sino que también el sistema utilizado para enviarlo y los sistemas que finalmente los recibieron[130]. Así también, es el caso de la mensajería instantánea utilizada en teléfonos a través de las funciones comunes de este, o de aplicaciones diseñadas para la mensajería instantánea como “WhatsApp”.

La evidencia que puede recogerse en el mundo digital de la informática puede presentarse en distintas formas, pero lo primordial en cuanto a esta, es que esta pueda ser recogida e interpretada por un funcionario, ya sea a través de sus conocimientos o de programas computacionales. Las evidencias digitales pueden llegar a tener ciertas características, como indica Patricia M. Delbono[131], estas evidencias pueden ser volátiles, anónimas, duplicables, alterables, modificables, y por último eliminables o suprimibles, estas características son importantes al momento de generar e interpretar estas evidencias, y reconocer su carácter maleable a la hora de extraer significado de estas.

Otro aspecto relevante a la investigación de la cibercriminalidad es la investigación en “la Nube”; la nube o “Cloud Computing” es una tecnología que permite el acceso de distintos servicios digitales a través de internet, permitiendo el uso de estos, acceso a aplicaciones, entre otros, permitiendo un acceso de manera remota a través de las tecnologías de la nube[132], el aspecto puramente digital que depende de servidores externos que mantienen un sistema digital, como una aplicación, una página web, foros,

---

[130] M. DELBONO, Patricia. “*Investigación Forense Sobre Medios Digitales*”. En: PARADA, Ricardo Antonio. “*Cibercrimen y Delitos Informáticos: Los nuevos tipos penales en la era de internet*”. Editorial Erreius. 1a edición. Argentina. Año 2018. p. 164. Disponible en: CIBERCRIMEN Y DELITOS INFORMÁTICOS

[131] M. DELBONO, Patricia. Ob Cit. p. 164. Disponible en: CIBERCRIMEN Y DELITOS INFORMÁTICOS

[132] HERRERA BRAVO, Rodolfo. “*Cloud Computing y Seguridad: Despejando Nubes para Proteger los Datos Personales*”. Revista de Derecho y Ciencias Penales Nº 17. Chile. Año 2011. p. 44. Recuperado de https://dialnet.unirioja.es/descarga/articulo/4200372.pdf

entre otros. Al requerir de acceso a servidores o sistemas privados que pueden o no tener relación con los delitos investigados, se requiere de autorización judicial para las diligencias realizadas sobre estas al tener este carácter privado.

Una herramienta utilizada, aunque no sea una tecnología novedosa, es la Identificación de Radiofrecuencias, un tipo de tecnología mediante la cual, "*se basa en la utilización de un pequeño chip que es adherido a un producto, lo que permite su rastreo y localización*."[133]Estos chips contienen información relevante respecto del producto u otros elementos, como lo han sido los documentos de identificación en Chile. Entonces, este elemento nos puede ayudar para determinar y descubrir dónde y cómo está siendo utilizado un objeto que cuente con esta tecnología, siempre y cuando se haga lectura del Chip utilizado.

La información debe ser leída para su utilización, los lectores se encuentran presentes en la locomoción pública, como metros y Transantiago, por supuesto, esta tecnología se utiliza para tarjetas de crédito que cuentan con un chip para identificación de radiofrecuencias. La presencia de este tipo de tecnología en las tarjetas utilizadas en por la población ha llevado a que puedan ser vulnerables a hackeos o a que sean accedidos los datos contenidos en estos chips[134], no solo eso, sino que la presencia de estos chips en teléfonos celulares ha llevado al mismo tipo de vulnerabilidades, a los que delincuentes pueden acceder y hacer uso de los datos contenidos para realizar delitos informáticos[135].

Los datos contenidos en los chips de identificación de radiofrecuencias pueden llegar a ser utilizados por delincuentes si estos acceden, tanto los datos personales, como los datos asociados a la funcionalidad del objeto que utiliza el chip, ya sea un teléfono celular, una tarjeta de crédito, etc., que pueden contener información acerca de las compras frecuentes de una persona, los datos de ingreso a los bancos asociados a la tarjeta, al igual que datos que pueden atentar contra la privacidad de la persona que está siendo víctima de la interceptación de sus datos, o del hackeo que puede haberse llevado a cabo.

---

[133] ASPIS, Analía. "*Identificación por Radiofrecuencia, Cibercrimen y Protección de Datos*". En: PARADA, Ricardo Antonio. "*Cibercrimen y Delitos Informáticos: Los nuevos tipos penales en la era de internet*". Editorial Erreius. 1a edición. Argentina. Año 2018. p. 144. Disponible en: CIBERCRIMEN Y DELITOS INFORMÁTICOS

[134] COLOMA, María. "*Gobierno acelera proyecto de ley contra delitos informáticos tras nuevas filtraciones de datos*". El Mercurio. Chile. 31 de agosto de 2018. Recuperado de: Gobierno acelera proyecto de ley contra delitos informáticos tras nuevas filtraciones de datos

[135] BBC News Mundo. "*Qué es el fraude "SIM swapping" y cuáles son las reglas de oro para evitarlo*". BBC News Mundo [en línea]. 10 de agosto de 2018. Disponible en: Qué es el fraude "SIM swapping" y cuáles son las reglas de oro para evitarlo - BBC News Mundo

Por tanto, a través del seguimiento del rastro que dejan estos elementos es que se puede dar con el paradero de la información utilizada, o incluso de elementos robados. Para esto se debe obtener acceso a las bases de datos que hacen uso de estos sistemas informáticos, para entonces analizar su uso. Las policías deben tener conocimiento de estos sistemas, sus comunes usos, y las formas en que se utiliza esta tecnología para cometer delitos, y así correctamente evitarlos e investigarlos.

Otro medio importante por considerar a la hora de la investigación a través de internet y de la nube es la de las "direcciones IP", estas son una forma de identificación única para cada persona en las redes de internet, la empresa de antivirus y protección informática Kaspersky la define como "*una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa "protocolo de Internet*", que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local"[136], por lo que prueba ser tremendamente útil al momento de identificar un usuario o participante anónimo y poder reconocer su actividad dentro del anonimato, aunque cambie su apariencia o nombre, al encontrarse siempre conectado a su dirección I.P. única para su dispositivo.

Por supuesto, no se puede ignorar que la dirección IP puede ser escondida, o al menos puede intentarse enmascararla, a través de programas y aplicaciones que lo permiten.

La dirección de IP puede ser rastreada, dejando registro de su uso en los sitios web varios de internet, y aunque, como explica Federico Borzi, la dirección de IP puede ser utilizada por una persona ajena al dueño de la computadora o dispositivo que utiliza dicha dirección, o incluso puede ser hackeada para su uso[137], los agentes policiales tienen diligencias para la obtención y su registro, con su debida autorización judicial, para obtener dichos registros de las empresas proveedoras de internet y adquirir así posibilidades de investigación. Es entonces la localización de direcciones de IP una de las herramientas fundamentales para las policías en cuanto a la investigación de ciberdelitos y en especial de los delitos informáticos, para formular el rastro y pasos que formaron parte del delito investigado.

Además de todo lo anterior, la policía de investigaciones cuenta con las herramientas comunes del Código Procesal Penal, que les permite, como se analizó

[136] Kaspersky. *Qué es una dirección IP: definición y explicación*. Página Web Kaspersky. Disponible en: Qué es una dirección IP: definición y explicación

[137] BORZI CIRILLI, Federico. "*Cibercrimen y Evidencia Digital: Problemática Probatoria*". En: PARADA. Ricardo Antonio. "*Cibercrimen y Delitos Informáticos: Los nuevos tipos penales en la era de internet*". Editorial Erreius. 1a edición. Argentina. Año 2018. p. 178. Disponible en: CIBERCRIMEN Y DELITOS INFORMÁTICOS.

anteriormente, acceder a comunicaciones privadas, correos electrónicos y en general a la interceptación de telecomunicaciones de todo tipo[138].

4.5.1 La “dark web” o “deep web”

La dark o deep web es una rama de las redes de internet, para la cual se requiere de navegadores especiales, distintos de los convencionales como Google, Firefox, entre otros. Debido a sus barreras de entrada informáticas y su peligro, la forma en que se obtienen los links de páginas web pertenecientes a la deep web son distintos también.

Estas redes de internet se utilizan para muchos objetivos inocuos y legales, pero también presenta actividad ilegal debido a la falta de regulación tanto interna como externa de estas páginas web, sumado a su dificultad de acceso y especial necesidad de protección, tanto de la dirección IP, como de la identidad real de la persona o funcionario que navega en esta.

Como se ha dicho anteriormente, el nivel de anonimato que se puede alcanzar a través del internet y sus páginas web y servidores es importante, pero también gradual, en el caso del uso de la deep web, su nivel de anonimidad es considerablemente más alto que en el caso de páginas web y servidores públicos[139].

En el uso común de internet, como ya se indicó al hablar de las herramientas de investigación, la navegación de cada persona es rastreada o rastreable personalmente a través de la dirección de IP. En ese sentido, lo que hace que el anonimato en la deep web sea tan efectivo es la falta absoluta de este elemento para la identificación de usuarios que utilizan esta vía, o al menos la capacidad de esconderla o prescindir de ella, las formas en específico para adentrarse en la deep web[140], navegar en esta y para lograr identificar usuarios dentro de esta puede llegar a ser relevante para la investigación de delitos, pero no será objeto de este trabajo de investigación.

Aprender a navegar en estos sitios web, al igual que tener las herramientas para identificar delitos, agentes delictuales y los medios utilizados para estos puede llegar a ser fundamental para reconocer, detener y procesar a los individuos por los delitos cometidos en esta forma sin regulación del internet.

---

[138] Chile. Congreso Nacional. Artículo 222 *Código Procesal Penal*. 2000

[139] TEMPERINI, Marcelo. “*Delitos Informáticos y Cibercrimen: Alcances, Conceptos y Características*”. En: PARADA, Ricardo Antonio. “*Cibercrimen y Delitos Informáticos: Los nuevos tipos penales en la era de internet*”. Editorial Erreius. 1a edición. Argentina. Año 2018. p. 64. Disponible en: CIBERCRIMEN Y DELITOS INFORMÁTICOS

[140] M. DELBONO, Patricia. “*Investigación Forense Sobre Medios Digitales*”. En: PARADA, Ricardo Antonio. “*Cibercrimen y Delitos Informáticos: Los nuevos tipos penales en la era de internet*”. Editorial Erreius. 1a edición. Argentina. Año 2018. p. 169. Disponible en: CIBERCRIMEN Y DELITOS INFORMÁTICOS

4.6 La investigación Internacional de ciberdelitos y delitos informáticos

Debido a la naturaleza de los ciberdelitos y de los delitos informáticos, los cuales son cometidos a través de internet, esto es, a través de páginas web, servidores, aplicaciones, etc., pertenecientes a distintos países, es que la doctrina ha establecido que se requiere para su investigación de la cooperación internacional, con el fin de lograr imputar y procesar a los ciberdelincuentes[141]. El internet permite a los ciberdelincuentes mantener cierto grado de anonimato permanente, lo cual dificulta su identificación, al igual que ocultan el país en el que residen, entre otros datos personales, pero también se dificulta la tarea de investigación puesto que, aunque se pueda detectar un delito, es posible que la víctima se encuentre igualmente en anonimato y no sea identificable[142].

Una forma para simplificar el problema de la internacionalización de los ciberdelitos es el de comprender la punibilidad de estos delitos como dependiente de donde son cometidos, o sea donde se encuentra la persona que comete el delito, o donde producen sus efectos, estas son dos teorías[143], esto puede llegar a solucionar el problema del uso de páginas web y servidores que pertenecen a otros países, aunque este tema no se encuentra actualmente zanjado por la doctrina, por lo que no nos servirá como base para determinar cómo funcionarán este tipo de delitos ni su investigación en concreto.

El uso de las herramientas antes nombradas permite la identificación de los autores de ciberdelitos y de delitos informáticos, los cuales, dependiendo de la gravedad del delito y la cuantía de la pena asociada puede llegar a solicitarse la extradición[144] del individuo para su procesamiento una vez este sea identificado.

---

[141] ROBLES CARILLO, Margarita. "*El ciberespacio: presupuestos para su ordenación jurídico - internacional*". Revista Chilena de Derecho y Ciencia Política. Vol. 7 N° 1. Chile. 22 de enero de 2016. pp. 8-9. Disponible en Vlex Chile

[142] MAYER LUX, Laura. "*Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos*". Revista Lux et Praxis. Nº 1. Año 2018. Chile. pp. 159-206. pp. 187-188. Disponible en: Vlex Chile

[143] CÁRDENAS ARAVENA, Claudia. "*El lugar de comisión de los denominados ciberdelitos*". Política Criminal. Chile. s.f. Disponible en: Vlex Chile

[144] Chile. Congreso Nacional. *Código Procesal Penal*, artículo 431. 2000

Conclusiones

A través de la investigación realizada sobre los delitos informáticos, el cibercrimen en general y, en especial, de la labor de la Policía , en específico de la Policía de investigaciones a través de su brigada especializada para la investigación de las formas delictuales descritas, es que podemos apreciar que, en primer lugar, la reciente Ley 21.459 sobre delitos informáticos trae consigo avances importantes para la determinación de los delitos informáticos, duplicando los tipos penales que poseíamos antes de la entrada en vigencia de esta Ley, logrando expandir los delitos comprendidos por la legislación chilena a estándares modernos, con la flexibilidad requerida en su lenguaje y figuras descritas para adecuarse igualmente a los avances tecnológicos e informáticos que pueden formular nuevos y más sofisticados tipos de delitos, para sus medios y formas de comisión,. Pero la nueva legislación no solo introduce avances en las formas que pueden adoptar los delitos informáticos, sino que de igual manera lleva consigo una nueva herramienta para la investigación de los delitos informáticos tipificados por la nueva ley, la del agente encubierto, que se suma a las herramientas que ya tienen nuestras policías para esta tarea.

También se exploraron y analizaron las diferentes herramientas y diligencias a las que tiene acceso el Ministerio Público para realizar a través de Carabineros y de la Policía de Investigación para la tarea de investigar delitos informáticos y el cibercrimen en general. Por esto, podemos decir que las herramientas y diligencias a las que tienen acceso nuestras policías son suficientes y eficientes para la investigación de los tipos delictuales descritos por la Ley de delitos informáticos, lo comprendido por la ciberdelincuencia y, que se encuentran preparados igualmente para las figuras delictivas que pueden desarrollarse en un futuro a través de las nuevas tecnologías que cada vez se hacen más frecuentes.

Podemos expresar entonces, que la especialización tanto legislativa, como en cuanto a los agentes policiales a la hora de investigar este tipo de delitos, es y ha sido suficiente para la correcta investigación de los delitos informáticos y, en general, de todo tipo de cibercrimen, y que por ende se encuentra preparada para el futuro de este tipo de delitos, y para la protección de los bienes jurídicos correspondientes a estos.

Se entiende que las características que presentan los delitos informáticos hacen que se presenten especiales dificultades para su investigación, por lo cual se requiere de la aplicación de métodos especiales y específicos para esta tarea, para lo cual los

agentes policiales requieren de preparación y especialización, debido a la diferencia para la investigación en comparación a otros delitos, como puede verse con las Brigadas Investigadoras de Cibercrimen de la PDI, que tienen funciones especiales y son específicamente utilizadas por el Ministerio Público debido a sus características de especialización y por contar con las herramientas necesarias para generar los insumos probatorios digitales, para su eventual análisis y comprensión del cual se puedan desprender rastros y evidencias que serán utilizadas en las causas penales asociadas a los delitos tratados en este trabajo de investigación.

Con todo esto, Carabineros, Policía de Investigación, el Ministerio Público, y en especial la Brigada contra el ciberdelito de la PDI se encuentran preparados y cuentan con los conocimientos y herramientas necesarias para la investigación del ciberdelito y en específico de los delitos informáticos, incluyendo así la nueva Ley 21.459.

Bibliografía

1. Alvarado Urízar, Agustina. "*El Control de la Resolución Motivada que Autoriza una Interceptación Telefónica en Chile y Duración de la Medida*". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso. XLIII. Chile. Año 2014. Disponible en: Vlex Chile

2. Álvarez Fortte, Héctor. "*Los Delitos Informáticos*". Revista Jurídica Regional y Subregional Andina. Edición 9°. Chile. Año 2009. Disponible en: Vlex Chile

3. ASPIS, Analía. "*Identificación por Radiofrecuencia, Cibercrimen y Protección de Datos*". En: PARADA, Ricardo Antonio. "*Cibercrimen y Delitos Informáticos: Los nuevos tipos penales en la era de internet*". Editorial Erreius. 1a edición. Argentina. Año 2018. Disponible en: CIBERCRIMEN Y DELITOS INFORMÁTICOS

4. BORZI CIRILLI, Federico. "*Cibercrimen y Evidencia Digital: Problemática Probatoria*". En: PARADA. Ricardo Antonio. "*Cibercrimen y Delitos Informáticos: Los nuevos tipos penales en la era de internet*". Editorial Erreius. 1a edición. Argentina. Año 2018. Disponible en: CIBERCRIMEN Y DELITOS INFORMÁTICOS.

5. Campos, Rodrigo "Capítulo II Normativa aplicable a los servicios de Cloud Computing utilizados por la administración del Estado". En: Jejina, Renato. *Derecho Informático*, 1era edición, Santiago, Chile: Editorial El Jurista, 2022. p: 299-301.

6. Canelo, Carola, Raúl Arrieta, Rodrigo Moya y Rodrigo Romo. "*El Documento Electrónico. Aspectos Procesales*". Revista Chilena de Derecho Informático. N°4, mayo de 2004 pp. 81-106. Disponible en: http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_simple/0,1493,SCID%253D15836%2526ISID%253D567%2526PRT%253D15830,00.html

7. Cárdenas Aravena, Claudia. "*El lugar de comisión de los denominados ciberdelitos*". Política Criminal. Chile. s.f. Disponible en: Vlex Chile

8. Cavada Herrera, Juan Pablo. "*Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera"*. Asesoría Técnico Parlamentaria. Chile. julio de 2020. Disponible en: Asesoría técnico parlamentaria

9. Cerda Santander, Claudio. "*Delitos informáticos crecen 74% en dos años y aumentan en casi todas las regiones*". El Mercurio. Chile. 8 de abril de 2018. Recuperado de Delitos informáticos crecen 74% en dos años y aumentan en casi todas las regiones

10. *Cibercrimen*, Policía de Investigaciones, 2020. Disponible en: Brigadas Investigadoras del Cibercrimen.

11. Chávez Chávez, Eric Andrés. "Décimo Grupo: Delitos Contenidos en Leyes Especiales". En: *Derecho Penal, Parte Especial*. Primera Edición. Tofulex, ediciones jurídicas. 2019. pp 709-713. Disponible en: Vlex Chile

12. Chile, *Moción Parlamentaria de Ley N° 19.223*, 16 de julio de 1991, Legislatura número 322, página 1. Disponible en Historia de la Ley N° 19.223.

13. Coloma, María. "*Gobierno acelera proyecto de ley contra delitos informáticos tras nuevas filtraciones de datos*". El Mercurio. Chile. 31 de agosto de 2018. Recuperado de: Gobierno acelera proyecto de ley contra delitos informáticos tras nuevas filtraciones de datos

14. Contreras Clunes, Alberto. "*Delitos Informáticos: un importante precedente*". Revista Ius et Praxis. V.9 n.1. Chile, Talca. Año 2003. Disponible en: Ius et Praxis II. JURISPRUDENCIA DELITOS INFORMÁTICOS: UN IMPORTANTE PRECEDENTE.

15. Consejo de Europa. "*Convenio sobre la ciberdelincuencia*". Budapest. 25 de octubre del año 2001. Disponible en: CONVENIO SOBRE LA CIBERDELINCUENCIA Budapest, 23.XI.2001

16. Cornejo Manríquez, Aníbal. "*Derecho Penal. Parte General y Especial en preguntas y respuestas*". 5° edición. Corman Editores Jurídicos. Año 2021. Disponible en: Vlex Chile

17. Cornejo Manríquez, Aníbal. "*Medicina legal, criminalística y criminología. Preguntas y respuestas*". 3a edición. Chile. Corman Editores Jurídicos. 2022. Disponible en: Vlex Chile

18. Cuervo Álvarez, José. "*Delitos informáticos: Protección Penal de la Intimidad"*. España. 2014. Disponible en: Delitos informáticos: Protección Penal de la Intimidad.

19. Diccionario Panhispánico del español jurídico. disponible en: Definición de cracker - Diccionario panhispánico del español jurídico - RAE

20. Duce J. Mauricio. "*Una aproximación empírica al uso y prácticas de la prueba pericial en el proceso penal chileno a la luz de su impacto en los errores del sistema"*. en Política Criminal. s.n. Disponible en Vlex Chile

21. Garrido Montt, Mario. "*Derecho Penal. Parte General. Tomo I*". Chile: Editorial Jurídica de Chile, 2010. Pgs 63-68. Disponible en: Vlex Chile

22. Garrido Montt, Mario. "*Derecho Penal. Parte General. Tomo I*". Chile: Editorial Jurídica de Chile, 2010. p 455. Disponible en: Vlex Chile

23. Herrera Bravo, Rodolfo. "*Cloud Computing y Seguridad: Despejando Nubes para Proteger los Datos Personales*". Revista de Derecho y Ciencias Penales Nº 17. Chile. Año 2011. p. 44. Recuperado de https://dialnet.unirioja.es/descarga/articulo/4200372.pdf

24. HORVITZ LENNON, María Inés y LÓPEZ MASLE, Julián. "*Derecho Procesal Penal Chileno II. Preparación del juicio, procedimientos especiales, ejecución de sentencias, acción civil*". s.n. Chile. Editorial Jurídica de las Américas. 2008. pp. 503-508. Disponible en: Vlex Chile

25. Kaspersky. *Qué es una dirección IP: definición y explicación*. Página Web Kaspersky. Disponible en: Qué es una dirección IP: definición y explicación

26. Maritano, Ana. "*Chile – Inauguran Cuartel Nacional de Cibercrimen*". Diario Jurídico [en línea]. Chile. 1 de noviembre de 2022. Disponible en: Chile – Inauguran Cuartel Nacional de Cibercrimen - Diario Jurídico

27. Maturana Miquel, Cristián. Montero López, Raúl. *Derecho Procesal Penal. Tomo I*. 1° edición. Chile. Abeledo Perrot Legal Publishing.

28. M. DELBONO, Patricia. "*Investigación Forense Sobre Medios Digitales*". En: PARADA, Ricardo Antonio. "*Cibercrimen y Delitos Informáticos: Los nuevos tipos penales en la era de internet*". Editorial Erreius. 1a edición. Argentina. Año 2018. Disponible en: CIBERCRIMEN Y DELITOS INFORMÁTICOS

29. MATUS ACUÑA, Jean Pierre; POLITOFF LIFSCHITZ, Sergio y RAMÍREZ G, María Cecilia. "*Lecciones de Derecho Penal chileno. Parte Especial*". s.n. Chile. Editorial Jurídica de las Américas. 2009. p 157. Disponible en: Vlex Chile

30. Mayer Lux, Laura. "*Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos*". Revista Lux et Praxis. Nº 1. Año 2018. Chile. pp. 159-206. Disponible en: Vlex Chile

31. Mayer Lux, Laura; Vera Vega, Jaime "*El documento como objeto material de las falsedades documentales y del sabotaje informático en el Derecho penal chileno*". Polít. crim. Vol. 14, Nº 27, julio 2019. Art. 12, pp. 419-455. Disponible en: http://politcrim.com/wp-content/uploads/2019/05/Vol14N27A12.pdf

32. Narváez, David. *El delito informático y su clasificación*, UNIANDES, Revista de Ciencia, Tecnología e Innovación, 2015, Vol. 2, Número 2, p. 158-173. Disponible en: El delito informático y su clasificación The computer crime and classification

33. Oxford Dictionaries [en línea]. Disponible en Oxford Learner's Dictionaries.

34. Núñez Vázquez, J. Cristóbal. "*Tratado del Proceso Penal y del juicio oral*". Tomo I. Chile. Editorial Jurídica de Chile. 2009. Disponible en: Vlex Chile.

35. Oxman, Nicolás. "*Estafas informáticas a través de internet: Acerca de la imputación penal del "Phishing" y el "Pharming"*". Revista de Derecho de la Pontificia Universidad Católica de Valparaíso XLI. Chile. 2013. Disponible en Vlex Chile

36. Policía de Investigaciones. "*Nuevo Complejo Policial contra el Cibercrimen*". Chile. 27 de octubre de 2022. Disponible en: Nuevo Complejo Policial contra el Cibercrimen

37. Real Academia Española [en línea]. Disponible en comerciar | Definición | Diccionario de la lengua española | RAE - ASALE

38. Real Academia Española [en línea]. Disponible en obstaculizar | Definición | Diccionario de la lengua española | RAE - ASALE

39. Robles Carillo, Margarita. "*El ciberespacio: presupuestos para su ordenación jurídico - internacional*". Revista Chilena de Derecho y Ciencia Política. Vol. 7 N° 1. Chile. 22 de enero de 2016. Disponible en Vlex Chile

40. Scheechler Corona, Christian. "*Aspectos fenomenológicos y políticos-criminales del sexting. Aproximación a su tratamiento a la luz del Código Penal chileno*". Política Criminal. Vol. 14, Nº 27 de julio de 2019. Disponible en Vlex Chile

41. Scheechler Corona, Christian. "*El childgrooming en la legislación penal chilena: sobre los cambios al artículo 366 quáter del código penal introducidos por la ley N° 20.526*". Revista Chilena de Derechos y Ciencia Política. Vol. 3, Nº 1. año 2012. pp. 55-78. Disponible en Vlex Chile

42. Temperini, Marcelo. "*Delitos Informáticos y Cibercrimen: Alcances, Conceptos y Características*". En: PARADA, Ricardo Antonio. "*Cibercrimen y Delitos Informáticos: Los nuevos tipos penales en la era de internet*". Editorial Erreius. 1a edición. Argentina. Año 2018. Disponible en: CIBERCRIMEN Y DELITOS INFORMÁTICOS.

43. *Unidades Especializadas*, Policía de Investigaciones,. Disponible en: Unidades Especializadas

44. Winter Etcheberry, Jaime. "*Elementos típicos del artículo 2° de la Ley Nº 19.223: Comentario a la SCS de 03.07.2013 Rol Nº 9238-12*". Revista Chilena de Derecho y Ciencias Penales. Vol. II, Nº 4. pp. 277-282. Disponible en: delito del artículo 2º de la ley nº 19.223 esPionaJe inforMático. bienes JurÍdicos Protegidos. aPoderaMiento, uso y conociM

Legislación Citada:

1. Chile, Congreso Nacional. artículo 2° *Ley N° 19.799*, 10 de octubre de 2014.
2. Chile. Congreso Nacional. *Código Penal*. 1874.
3. Chile. Congreso Nacional. *Código Procesal Penal*. 2000.
4. Chile. Congreso Nacional. Decreto Ley 2460 del 9 de enero de 1979.
5. Chile. Congreso Nacional. Ley *N° 19.223* del 7 de junio de 1993.
6. Chile. Congreso Nacional. *Ley N° 20.000* de 16 de febrero de 2005.
7. Chile. Congreso Nacional. *Ley N° 21.459*, 20 de junio de 2022. Disponible en: Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos
8. Chile. Congreso Nacional. Ley orgánica Constitucional de Carabineros 18.961 de 7 de marzo de 1990.

Jurisprudencia Citada:

1. Cuarta Sala de la Corte de Apelaciones de Concepción. Sentencia de la causa Resolución nº 9440 de la Causa nº 844 del año 2014. Disponible en: Vlex Chile
2. Primera Sala de la Corte de Apelaciones de Copiapó. Resolución nº 15 de la Causa nº 448 de 2018. 19 de diciembre de 2018 Disponible en: Vlex Chile
3. Segunda Sala de la Corte Suprema. Resolución nº 8042-2009. 25 de enero de 2010. Disponible en: Vlex Chile