76

COLECCIÓN
MATERIALES
DOCENTES

Criminalidad informática y ciberdelincuencia

Marta Herrera Seguel
Ymay Ortiz Pulgar

ACADEMIA JUDICIAL CHILE

2024

Marta Herrera Seguel

Abogada de la Universidad de Chile, master of laws por California Western School of Law, San Diego, California, Estados Unidos. Profesora de Derecho Procesal de la Universidad de Santiago de Chile y de la Universidad Finis Terrae, y codirectora del Diplomado en Derecho Penal Económico de la Universidad Adolfo Ibáñez. Durante dieciséis años fue directora jurídica y directora de la Unidad Especializada Anticorrupción de la Fiscalía Nacional del Ministerio Público, y en la actualidad es fiscal y encargada de Seguridad de la Información en el Instituto Nacional de Propiedad Industrial.

Ymay Ortiz Pulgar

Abogada de la Universidad de Chile y magíster en Derecho Penal por la Pontificia Universidad Católica de Valparaíso. Cuenta con un postítulo en Justicia Criminal y Sistema Acusatorio de la Universidad Diego Portales. Profesora de Derecho Penal en el Máster de Derecho y Género de la Universidad de Jaén y el Instituto de Estudios Judiciales. Ejerce como abogada litigante en materias penales y durante veintidós años se desempeñó en el Ministerio Público, dieciocho de ellos como fiscal adjunta y los restantes como directora de la Unidad Especializada en Derechos Humanos, Violencia de Género y Delitos Sexuales de la Fiscalía Nacional del Ministerio Público.

ACADEMIA JUDICIAL CHILE

Criminalidad informática y ciberdelincuencia
MATERIALES DOCENTES 76

Amunátegui 465, Santiago de Chile
academiajudicial.cl • info@academiajudicial.cl

ISBN: 978-956-08163-9-9

EDICIÓN Y DISEÑO: DER Ediciones | derediciones.com

Resumen

Bajo el título *Criminalidad informática y ciberdelincuencia*, este material docente incorpora los distintos aspectos propios de esta categoría delictiva. Para ello hemos comenzado relevando el fenómeno que las tecnologías de la información y las comunicaciones representan en la vida diaria de las personas y, por ende, también en materia de comisión de delitos, los que pueden verse facilitados por el auge del desarrollo tecnológico.

Luego se analiza cada uno de los tipos penales contemplados en la nueva legislación sobre delitos informáticos, así como los ya existentes en otros cuerpos normativos, junto con otras disposiciones relevantes en materia sustantiva, como las circunstancias modificatorias de responsabilidad penal. Posteriormente, se abordan los aspectos procesales, con la particularidad de que, en el campo de la prueba electrónica, la referencia es general y no solo para los delitos informáticos. Ello, por cuanto hemos tomado como referencia fundamental para este trabajo la normativa contenida en el Convenio de Budapest, al cual nuestra legislación ha debido ajustarse en el marco de la Ley de Delitos Informáticos, lo que incluye cualquier ilícito que pueda probarse por evidencia digital.

Contenido

Introducción

Este material docente intenta presentar los aspectos esenciales asociados a esta especial forma de criminalidad, la ciberdelincuencia. No se trata de un análisis exhaustivo de la parte sustantiva ni procesal de esta categoría delictiva, cuestión que excedería el objetivo de este trabajo, sino que solo pretendemos exponer sistemáticamente las disposiciones vigentes, tanto las incorporadas por la reciente legislación como las ya existentes en materia de ciberdelincuencia, incluyendo, por cierto, la normativa de carácter internacional y aludiendo a la lógica tras esas disposiciones.

Por ello hemos abordado, en primer lugar, los aspectos generales asociados a la ciberseguridad y la ciberdelincuencia, delimitando el marco normativo existente y las razones que han llevado a adoptar rápidamente una legislación que se adapte a la necesidad de todas las personas de vivir en un entorno cibernético seguro y respetuoso de nuestros derechos.

En un segundo capítulo, nos abocamos al análisis de los aspectos penales involucrados en materia de ciberdelincuencia, lo que implica detenerse particularmente en la Ley 21.459 y los nuevos tipos penales que reemplazaron la desactualizada regulación de la Ley 19.223. Pero, además, se alude a figuras ya existentes y lamentablemente de bastante ocurrencia, como las de *phishing* y *pharming*, o aquellas vulneratorias de la indemnidad sexual de niños, niñas y adolescentes que se cometen aprovechando las debilidades que ofrece el espacio virtual. También se hace referencia a otros aspectos propios del derecho penal sustantivo, como las circunstancias modificatorias de responsabilidad penal.

El marco sustantivo, para ser útil, requiere de un apropiado escenario procesal que permita que las investigaciones penales puedan desarrollarse adecuadamente y se pueda cumplir el objetivo de los Estados de resguardar apropiadamente los derechos de las personas. Por ello, en el capítulo III, abordamos los aspectos procesales con la particularidad de que, en este caso, no nos limitamos a la investigación y juzgamiento

de los delitos informáticos, sean los definidos en la Ley 21.459 o en la normativa previa, sino que se abordan –limitadamente, por cierto– los desafíos que trae aparejada la prueba electrónica tanto para esta categoría delictiva como para cualquiera, dado que pruebas digitales podemos encontrar para todas ellas.

Finalmente, sobre la base de que ni los delitos informáticos ni la evidencia digital que generan estos y otros delitos reconocen frontera alguna, en el entendido de que no solo vivimos y actuamos en un mundo globalizado, sino que la transnacionalización cobra más vigor en esta materia delictiva que en cualquier otra, en el último capítulo desarrollamos los aspectos propios de la cooperación internacional en lo que respecta a Chile, regulado por el Convenio sobre Ciberdelincuencia del Consejo de Europa.

Las autoras agradecen la formación proporcionada por el Consejo de Europa, que contribuyó a la redacción de este material.

Esperamos que los contenidos que expondremos, junto a los ejemplos que entregaremos, resulten de utilidad a lectores y lectoras para avanzar en el conocimiento y comprensión de una materia particularmente técnica como la ciberdelincuencia.

Capítulo 1

Introducción a la ciberdelincuencia

1. Importancia de la ciberseguridad en el mundo actual

El concepto de ciberespacio fue utilizado por primera vez en el año 1984, en la novela futurista *Neuromante*, de William Gibson. Con el surgimiento de la World Wide Web en el año 1990, ese espacio virtual fue bautizado con este término.

Posteriormente, y con la masificación de la Internet tras la liberación para explotación comercial de las redes de telecomunicaciones en el año 1995, el número de personas que accedían a la web a través de Internet creció de manera explosiva, junto con una nueva industria y mercado: la computación y una incesante producción de plataformas tecnológicas destinadas a diversos usos y prestación de servicios.

En esta misma época se hizo común la utilización del concepto de «ciberespacio» en referencia a una realidad o espacio virtual presente en todos los ordenadores y las redes mundiales de computadoras.

Su definición alude a un espacio de tipo «virtual», vale decir, conforme a la Real Academia Española (en adelante, RAE), se trataría de un espacio *aparente, inexistente físicamente*. Sin embargo, la relevancia que fue adquiriendo el ciberespacio o espacio virtual acerca cada vez más la definición de este concepto a su raíz latina *virtus* o *virtuale*, es decir, al concepto de facultad, fuerza, virtud. Y es que resulta difícil negar la existencia de un lugar donde las personas interactúan de manera cada vez más cotidiana y con mayor intensidad.

Durante los últimos treinta años de manera exponencial y luego exacerbada con la pandemia del COVID-19, que obligó a una confinación masiva a nivel mundial, una parte cada vez más relevante de la existencia de la humanidad se desarrolla por medios digitales o virtuales. Así, a través de plataformas tecnológicas o digitales, las personas producen y adquieren bienes y servicios, interactúan, realizan sus transacciones financieras, comercializan, se comunican, desarrollan sus afectos, estudian, trabajan, se divierten, revisan aspectos asociados a su salud, etc.

En efecto, podemos pensar en múltiples actividades realizadas permanentemente a través de esta vía e incluso, aunque no tenga mucha cabida en nuestro país a consecuencia del buen funcionamiento de nuestro sistema electoral, la propia decisión de quienes nos representan y ejercen el poder podría quedar radicada, en buena medida, en sistemas informáticos, como ocurre en todos aquellos países que cuentan con sistema de voto electrónico.

Esta trascendencia motivó que el 8 de febrero de 1996 el poeta, ensayista y ciberactivista estadounidense John Perry proclamara, en Davos, Suiza, la Declaración de Independencia del Ciberespacio, respecto del cual ninguna persona o gobierno debería ejercer soberanía, definiendo al ciberespacio como «El nuevo hogar de la mente». Considerando que la cuestión jurisdiccional es uno de los problemas que plantea la realidad actual, cobra sentido aquella declaración.

Este desarrollo tecnológico genera enormes posibilidades y una transformación de las sociedades contemporáneas que era imposible prever hace tan solo algunos años y que en un futuro próximo podría superar hasta la más imaginativa novela de ciencia ficción.

Como parte de la estructura social, el derecho se ha visto impactado *en todas sus expresiones* e incluso ha surgido una nueva rama jurídica, el *derecho informático*.

Pero la ampliación en el plano normativo se ha ido extendiendo desde un tímido derecho informático a diversas ramas del derecho que, de un modo u otro, se han visto afectadas por las nuevas tecnologías, generando una expansión que excede el plano del original derecho informático y que va exigiendo su adaptación a distintos ámbitos. Todo ello es bastante natural, porque lo que ocurre en el plano jurídico corresponde exactamente a lo que pasa en la vida diaria: los más diversos ámbitos de la vida se han visto impactados por los desarrollos tecnológicos de manera creciente y acelerada, lo que sin duda nos reporta una serie de beneficios, nos facilita accionar en distintos planos, pero, de otra parte, nos genera una serie de riesgos y, por tanto, de desafíos que resulta indispensable abordar de forma adecuada.

En consecuencia, es el Estado el que adquiere el deber de proteger la información que las personas entregan al ciberespacio, cuidando así tanto la confianza que la ciudadanía deposita en sus autoridades, como la serie de bienes jurídicos de la población que se pueden ver afectados en el plano virtual, de modo tal que no somos ya solo los ciudadanos y

ciudadanas individualmente considerados quienes debemos prever que los riesgos no se materialicen, sino que es el propio Estado el que debe darnos garantías de aquello.

De hecho, cuando el Estado no actúa en materia de ciberseguridad, los derechos, el patrimonio y la seguridad de las personas se ven afectados, por lo que ha sido importante que el Estado entienda que no está protegiendo computadores, sino personas, sus bienes, su intimidad, su seguridad, etc., y la sociedad en su conjunto.

Una muestra clara de la afectación masiva de este tipo de conductas se ha hecho conocida recientemente, el 23 de octubre de 2023, con el ataque que sufrió la empresa GTD,[1] que fue calificado como «un incidente grave […] masivo» por la Agencia de Ciberseguridad del Gobierno (CSIRT[2]), que afectó durante casi un mes a miles de empresas y servicios del Estado, y originó una investigación penal por delito informático y la interposición de, al menos, dos acciones constitucionales de protección por los daños generados a los clientes de GTD como consecuencia del ciberataque.

En cuanto al derecho penal, las transformaciones tecnológicas y esta nueva realidad virtual han facilitado o provisto de nuevas herramientas y formas de atentar y amenazar diversos bienes jurídicos tradicionalmente protegidos, como la propiedad, la intimidad, la seguridad y la fe pública, la indemnidad y libertad sexual, etc., así como otros bienes jurídicos necesitados de protección jurídico-penal, que han surgido y seguirán surgiendo derivados de esta vertiginosa evolución tecnológica.

Inicialmente, los delitos cometidos a través de diversos dispositivos de almacenamiento y transmisión de datos que atentaban contra bienes jurídicos tradicionales se calificaron con figuras penales ya reguladas, como hurto, falsificación, amenazas, etc. Sin embargo, la evolución delictiva avanza en paralelo a la tecnológica, explorando y apropiándose de cada nueva tecnología. Lo anterior desafía a los países a mantener en constante cambio su legislación para evitar espacios de impunidad y tratar de prevenir futuros delitos.

Precisamente la calificación de «informáticos» de este tipo de delitos deriva, por una parte, de que la utilización de la tecnología es el medio para cometerlos, aprovechando la inmediatez y el anonimato de Inter-

1 Troncoso (2023), s.p.; CNN Chile (2023), s.p.
2 Por las siglas de *Computer Security Incident Response Team.*

net, y, por otra, de que el daño, vulneración, afectación, destrucción o intromisión de los dispositivos de almacenamiento o transmisión de datos suele ser su objetivo.

Una percepción muy extendida es que quienes cometen estos delitos son personas expertas y con conocimientos tecnológicos o informáticos que les permiten ingresar a sistemas muy complejos de almacenamiento de datos. En algunos tipos de delitos es así, como en aquellos que implican el acceso a dispositivos o sistemas de almacenamiento que contienen grandes volúmenes de información, como los bancos, servicios estatales, etc. En otros casos, es un programa o dispositivo de acceso cuya utilización se ha masificado en el ambiente criminal y cualquiera lo puede utilizar, como, por ejemplo, los fraudes bancarios, ejecutados incluso por personas privadas de libertad, o la explotación sexual de niños y niñas por parte de agresores que utilizan la web para conectar a las víctimas o para difundir sus imágenes, con un conocimiento básico que les permite crear un perfil de una red social.

Una característica única de los delitos que ocurren o se realizan en el espacio virtual es que los conceptos de espacio y tiempo se desdibujan respecto de los espacios físicos, desafiando tanto la relación de las víctimas con los agresores como los conceptos de prueba o evidencia, sitio del suceso, competencia, jurisdicción, etc.

De manera muy simple, la realidad o espacio virtual es la actividad y estímulos eléctricos de los dispositivos informáticos a través de los cuales se trasmite y procesa información, creando estructuras emergentes (patrones) que evolucionan a lo largo del tiempo en lo que llamamos espacio virtual.

A su vez, Internet es un conjunto descentralizado de redes de comunicación a través de protocolos; el ciberespacio es el lugar en el que se producen las comunicaciones de Internet. Ambos conceptos son distintos a pesar de que suelen presentarse como sinónimos y no es posible entenderlos de manera separada.

En consecuencia, la prueba o evidencia digital está conformada por los datos y la información que transmite, recibe y/o almacena un dispositivo informático y el sitio del suceso ya no estará definido por las reglas de las dimensiones físicas.

Esta evidencia posee características propias: es inmaterial, ya que se trata de impulsos eléctricos procesados por un dispositivo; es frágil, ya que puede ser fácilmente dañada, modificada o perdida, lo que obliga a

generar constantemente mejoras en los sistemas de almacenamiento; es volátil, ya que algunos datos son de naturaleza transitoria y se eliminan automáticamente del dispositivo que los aloja, y fácilmente ocultable, ya que puede almacenarse en otros dispositivos, como *pendrives* o discos externos.

Asimismo, la utilización de la mayoría de los dispositivos informáticos solo requiere un nombre de usuario y una contraseña que puede estar totalmente desvinculada de la persona que está utilizando el dispositivo, facilitando el anonimato de quienes cometen delitos informáticos.

Por último, y con relación a la definición de lo que tradicionalmente se ha entendido como «el lugar en que se cometió o comenzó a ejecutarse el delito», la cuestión es mucho más compleja. Cualquier persona puede operar su dispositivo en un determinado lugar y causar efectos inmediatos en otra persona o dispositivo ubicado en otro país, utilizando una empresa prestadora del servicio de Internet con domicilio legal en un tercer país y que, a su vez, mantiene sus servidores de almacenamiento en un cuarto país.

Lo anterior ha requerido desarrollar conocimientos profesionales y herramientas tecnológicas especiales, así como también legales, que permitan adquirir, preservar y analizar la evidencia en tiempo y forma, ya que la manipulación inadecuada de los sistemas involucrados en un delito, y la dilatación del tiempo transcurrido entre la comisión del delito y la adquisición de la evidencia, pueden destruirla o alterarla significativamente, imposibilitando el avance de la investigación.

A nivel internacional, y dadas las características de anonimato, inmediatez y transaccionalidad que hemos descrito respecto de los delitos que ocurren en el ciberespacio, los países se han visto en la necesidad de hacer acuerdos en cuanto a la penalización, investigación y colaboración en la investigación y juzgamiento de estos delitos.

Por último, otra de las características de estos delitos es la cifra oculta respecto de su ocurrencia.

Dentro de las causas que afectan la denuncia de estos delitos, podemos encontrar el desconocimiento de las víctimas de que están siendo atacadas, falta de motivación por la existencia de seguros que cubren el riesgo de estos ataques, falta de confianza en que la justicia podrá investigar e identificar al autor de estos delitos y, en el caso de las empresas, por la pérdida de prestigio que trae el reconocimiento de que sus sistemas de seguridad informáticos han sido vulnerados.

En el desarrollo de este trabajo pretendemos entregar las herramientas suficientes para entender la complejidad de los delitos informáticos, tanto de aquellos tradicionales en que la tecnología es un medio de optimización de recursos como de aquellos cuyo objetivo es el ataque a los sistemas o dispositivos informáticos.

2. Derecho y nuevas tecnologías

La inmersión en las nuevas tecnologías ha sido tan vertiginosa e intensa que, probablemente, no hemos dimensionado aún su impacto completo. Las tecnologías de la información y de las comunicaciones (TIC) influyen en las formas de organización social que se pueden desarrollar en cualquier periodo histórico; en gran medida, ellas impulsan la historia, ya que los atributos tecnológicos particulares de un medio o de una mezcla de medios prevalentes en una determinada sociedad condicionan la práctica de la comunicación en esa sociedad, las instituciones y los acuerdos socioculturales que se asocian con esas prácticas, y a través de ellas los acuerdos más generales entre las sociedades y los climas culturales.[3]

La tecnología es una extensión de la persona moderna, de igual modo en que un utensilio de piedra era la extensión de la mano del hombre primitivo; la mayoría de los avances tecnológicos son intentos de extender la capacidad física del ser humano. Sin embargo, las tecnologías de la información y de las comunicaciones son una extensión del pensamiento, de la consciencia, de las capacidades perceptivas únicas del ser humano, y de esta forma, son una extensión de su mente.

Así, podemos hablar de que estamos en presencia de una nueva *era digital*, que implica una revolución transcendental como otras en la historia de la humanidad, por lo que difícilmente podría relegarse el campo de lo normativo únicamente al derecho informático, sino que más bien se trata de hacer el planteamiento radicalmente inverso, que comience por cuestionarse si existe algún ámbito del ordenamiento jurídico –e incluso de la vida misma– que pueda estar ajeno al fenómeno tecnológico.

En efecto, en esta nueva era digital, han surgido cuestiones como la firma electrónica; la tutela de la intimidad y el régimen de protección de los datos de carácter personal; la disciplina de los servicios de la sociedad de la información; la protección de la intimidad de traba-

3 Aranda (2020). P. 38.

jadores y trabajadoras y los problemas planteados por el teletrabajo; el régimen de las relaciones telemáticas con la Administración Pública, así como las iniciativas de democracia electrónica; el cambio radical de coordenadas que la revolución tecnológica comporta en el campo de la propiedad intelectual; el régimen jurídico de los nombres de dominio; la criminalidad informática; los problemas de jurisdicción competente y de ley aplicable derivados de la naturaleza global de la red; los aspectos tributarios del comercio electrónico, entre otros.

De esta forma, las nuevas tecnologías han tenido gran influencia en múltiples campos del derecho, dado que han afectado nuestra vida en general. Así, las nuevas tecnologías han influido desde el derecho laboral o penal hasta el surgimiento de nuevos campos y tecnologías.

En el ámbito del derecho laboral, por ejemplo, la aparición de nuevas formas de trabajo como el teletrabajo, y la influencia de las tecnologías en el control de la actividad laboral y en el uso de ciertas herramientas tecnológicas son aspectos con los que el derecho ha de enfrentarse.

También es cada vez más importante la *protección de datos*, debido a que el uso creciente de las TIC, redes sociales e Internet ha creado situaciones de riesgo que afectan de forma grave la esfera personal de ciudadanos y ciudadanas.

El comercio electrónico también supone un reto para el sector legal debido al aumento significativo tanto de las compras realizadas por Internet como de sitios web y empresas que ofrecen bienes y servicios desde cualquier parte del mundo.

Relacionado con el comercio electrónico, las nuevas tecnologías también han tenido un gran impacto en el consumo, la publicidad y la competencia desleal, aspectos que el derecho debe proteger con sumo cuidado, en beneficio de las personas consumidoras, teniendo en cuenta que vivimos en una sociedad global y de la información… o de la desinformación, en muchas ocasiones.

En conclusión, cuando hablamos de delitos informáticos, no estamos hablando de ninguna cuestión excepcional, sino de una lógica consecuencia de la materialización de los riesgos más intensos que puedan ocasionarse para la vida en sociedad en el marco de una actividad presente en todo tiempo y lugar.

3. Diagnóstico preliminar en materia de ciberseguridad

De todo lo anteriormente expuesto surge la necesidad de que el Estado afronte directamente la cibercriminalidad y, de una forma más amplia, se haga cargo de la necesidad de establecer mecanismos potentes en materia de ciberseguridad, cuestión que se ha planteado ya desde hace unos años y ha tenido un desarrollo muy importante –aunque seguramente insuficiente– en la actualidad.

La creciente evolución del fenómeno hace imprescindible evaluar lo que el Estado de Chile y la sociedad están haciendo en materia de ciberseguridad. Según el reporte sobre Ciberseguridad de la Organización de los Estados Americanos (OEA) de 2020, que considera cinco dimensiones: política, cultural, formación, marco regulatorio y técnica, Chile tiene un nivel de madurez intermedio en este terreno.

Como Estado contamos con el Comité Interministerial sobre Ciberseguridad y la Coordinación Nacional de Ciberseguridad, además de un instrumento: la *Política Nacional de Ciberseguridad*, en adelante PNCS.

La PNCS, elaborada en el gobierno de la presidenta Michelle Bachelet, fijó los lineamientos políticos del Estado de Chile para el resguardo de la seguridad de las personas y de sus derechos en el ciberespacio. En el gobierno del presidente Sebastián Piñera, se confirmó la PNCS como una política de Estado, se avanzó en su implementación y presentó un Proyecto de Ley Marco sobre Ciberseguridad.

Con fecha 4 de diciembre de 2023, se publicó en el Diario Oficial la *Política Nacional de Ciberseguridad 2023-2028*, aprobada mediante Decreto 164 del Ministerio del Interior y la Seguridad Pública, suscrito en Santiago, con fecha 16 de junio de 2023, conforme a lo dispuesto en el artículo 1° de la Ley 20.502. La resolución se funda en que, durante los últimos años, las TIC han asumido un rol fundamental en la manera de desenvolvernos como sociedad. La consolidación de este mundo digital ha traído múltiples oportunidades efectivas de bienestar y crecimiento tanto social como económico; sin embargo, este tejido digital es frágil, porque implica inevitablemente una serie de riesgos y amenazas para la seguridad de las personas.

En su numeral 3 sostiene: «Que, nuestro país enfrenta desafíos importantes en la materia, teniendo un nivel medio de madurez en comparación al resto del escenario internacional, conforme lo indica el Índice Mundial de Ciberseguridad de la Unión Internacional de Telecomuni-

caciones. En el Índice Mundial de Ciberseguridad del año 2020, Chile se encuentra en el lugar 74 a nivel mundial, y en el 7° lugar en América (debajo de Estados Unidos, Canadá, Brasil, México, Uruguay y República Dominicana). En este índice, Chile se destaca por su avance en medidas legales, medidas organizacionales y de cooperación; sin embargo, se queda atrás en el ámbito técnico. En el Índice Nacional de Ciberseguridad, desarrollado por Estonia y actualizado de forma continua, Chile se encuentra al año 2023 en el lugar 53 entre 175 países, y en el 6° lugar en Latinoamérica y el Caribe, debajo de República Dominicana, Argentina, Paraguay, Perú y Uruguay. En este *ranking*, que consta de 12 áreas distintas, Chile se destaca en desarrollo de políticas de ciberseguridad, lucha contra el cibercrimen y operaciones militares; pero se queda atrás en protección de servicios esenciales, protección de servicios digitales, gestión de crisis y protección de datos personales».[4]

La Política enuncia los principales problemas que Chile enfrenta hoy en materia de ciberseguridad:

Y, a su vez, define los cinco objetivos de la Política Nacional de Ciberseguridad:

1. La posibilidad de contar con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad y de desastres socioambientales, bajo una perspectiva de gestión de riesgos.
2. La protección y promoción de los derechos de las personas en Internet.
3. El desarrollo de una cultura de ciberseguridad en torno a la educación, buenas prácticas, responsabilidad en el manejo de tecnologías digitales, y promoción y garantía de los derechos de las personas.
4. La creación de una gobernanza pública para coordinar las acciones necesarias en ciberseguridad nacional e internacionalmente.
5. El fomento a la industria y la investigación científica, protegiendo a las personas y las organizaciones, y que sirva a los objetivos estratégicos de la industria y la investigación.

4 Diario Oficial de la República de Chile. Edición 43.717, de 4 de diciembre de 2023. Normas Generales, CVE 2415658. Ministerio del Interior y la Seguridad Pública. Subsecretaría del Interior. Aprueba Política Nacional de Ciberseguridad 2023-2028. Número 164. Santiago, 16 de junio de 2023.

Adicionalmente, la política incluye algunas dimensiones transversales con las que se busca proteger y promover la protección de los derechos de las personas y sus familias en Internet: la equidad de género, la protección al adulto mayor y la protección del medio ambiente.

Dentro de las acciones que se contemplan para lograr el primer objetivo, esto es, el de contar con una infraestructura de la información robusta y resiliente en materia de ciberseguridad, se encuentra la reciente Ley 21.663, Marco sobre Ciberseguridad, publicada y vigente desde el 8 de abril de 2024, cuyo objetivo es robustecer al país en materia de ciberseguridad. Para esto, la iniciativa establece una institucionalidad que contará con una Agencia Nacional de Ciberseguridad, y principios y normativa general para estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado. Asimismo, la institucionalidad coordinará las acciones de los organismos del Estado con particulares.

La nueva normativa establece requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad. Por otro lado, señala las atribuciones y obligaciones de los organismos del Estado. Y, además, define los deberes de las instituciones privadas y los mecanismos de control, supervisión y responsabilidad ante infracciones. En resumen, se trata de una institucionalidad que pretende velar por la protección, promoción y respeto del derecho a la seguridad informática de las personas y sus familias.

4. Deberes del Estado en materia de protección de la seguridad de los ciudadanos

Como constata la actual PNCS, Chile se destaca por su avance en medidas legales, medidas organizacionales y de cooperación, de modo que paulatinamente se va completando el marco jurídico apropiado para que podamos contar con una regulación acorde a la realidad tanto en materia de ciberseguridad como de ciberdelincuencia, y ello no es menor si atendemos a la constante evolución de estas materias y, consecuentemente, el esfuerzo de seguimiento y actualización que se exige por parte de la autoridad, que en más de una ocasión hará que, no obstante los esfuerzos realizados, el marco normativo se vea desfasado en comparación con la realidad.

De allí que surge la necesidad de generar un estructura adecuada para hacerse cargo de las necesidades existentes en materia de ciberseguridad, de forma que, mediante Resolución Exenta 5.006 del Ministerio del Interior y Seguridad Pública, de 20 de agosto de 2019, pero con vigencia operativa desde el 3 de septiembre del mismo año, se formaliza la creación del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés: *Computer Security Incident Response Team*) como un departamento dentro de la estructura del gobierno, específicamente en la Subsecretaría del Interior y Seguridad Pública. El nuevo equipo asume funciones que, hasta esa fecha, eran desempeñadas dentro de la Red de Conectividad del Estado (RCE).

El CSIRT define su visión como la de contar con un ciberespacio libre, abierto, seguro y resiliente. Y su misión es fortalecer y promover buenas prácticas, políticas, leyes, reglamentos, protocolos y estándares de ciberseguridad en los órganos de la Administración del Estado, las infraestructuras críticas del país y la República de Chile en su conjunto, para que el proceso de transformación digital de cara a los ciudadanos se consolide con la mayor seguridad posible, sustentado tanto en el desarrollo de un ecosistema digital seguro y resiliente, como en la creación de una capacidad de respuesta –preventiva, reactiva y proactiva– a los incidentes de ciberseguridad que afecten su integridad, disponibilidad o confidencialidad.

Sus objetivos son:

- Proveer información y asistencia a la Red de Conectividad del Estado y, en general, al ciberespacio gubernamental.
- Administrar un sistema de cooperación nacional e internacional en materias de ciberseguridad, con el objetivo de reducir los riesgos y articular la respuesta ante estos cuando su materialización sea efectiva.
- Promover buenas prácticas en materia de ciberseguridad en la Administración gubernamental.
- Promover la protección de las infraestructuras de información críticas del país (CIIP, por sus siglas en inglés) y recursos claves.
- Promover el fortalecimiento del marco jurídico en lo que se refiere a delitos informáticos y cibercrimen.
- Promover la concienciación en materias de ciberseguridad.

Su alcance comprende los ministerios, las intendencias, las gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública, los gobiernos regionales, las municipalidades y las empresas públicas creadas por ley.

El sector privado se integra a la cobertura en la medida que pertenezca a sectores estratégicos o se haya establecido un convenio de colaboración público-privado,[5] lo que resulta plenamente consistente con el contenido de la nueva Ley 21.663.

Como puede apreciarse de los objetivos definidos para esta nueva estructura, ellos incorporan un rango de materias bastante extenso que va desde la Red de Conectividad del Estado hasta los delitos informáticos y, en caso de realizarse una evaluación, probablemente podría advertirse que su campo de acción es bastante más amplio que la dotación efectiva de personas necesarias para hacerse cargo de las funciones que comprende. Por cierto, el contexto está dado no solo por este equipo humano, sino por un marco jurídico compuesto por diversos cuerpos legales o normas de rango infralegal que apuntan a regular la materia, algunas de las cuales referiremos en este trabajo.

5. Deberes en relación con la protección de los datos personales (artículo 19 número 4 CPR)

Un tema central en materia de los riesgos que conlleva la cibercriminalidad, en cualquiera de sus acepciones, está constituido por los atentados contra los datos personales, cuya protección ha sido elevada a rango constitucional con la Ley 21.096, que consagra el derecho a protección de los datos personales modificando el artículo 19 número 4 de la Constitución Política de la República, a fin de incorporar este derecho fundamental que se ve amenazado frecuentemente en el llamado «ciberespacio».

No obstante haberse introducido esta importante modificación a la Carta Fundamental, ella no ha podido, a la fecha, materializarse en rango legal con la modificación a la Ley 19.628, pese a que, desde el año 2017, se encuentra en tramitación el Proyecto de Ley contenido en los Boletines 11144-07 y 11097-07, fusionados. Actualmente, dicho Proyecto

5 CSIRT (s.f.), s.p.

se encuentra en el Tribunal Constitucional luego de que, con fecha 26 de agosto de 2024, el Congreso Nacional aprobara el texto que modifica la Ley 19.628, elevando el estándar de protección de los datos personales en Chile, y creando la Agencia de Protección de Datos Personales. Esta ley entrará en vigencia veinticuatro meses después de su publicación, con el objeto de dar tiempo a las organizaciones a prepararse para las exigencias que impone la nueva normativa.

En el mensaje con que se inicia la tramitación parlamentaria de este proyecto se lee que «La sociedad digital ha expandido los espacios de libertad, autonomía y desarrollo de las personas, pero también ha diseñado nuevos y sofisticados sistemas de control y vigilancia que amenazan o limitan esa misma libertad. Parte importante de los desafíos que actualmente enfrentan las sociedades y los gobiernos es crear reglas de conducta que permitan organizar las transformaciones en la sociedad digital. Se trata de diseñar instituciones, marcos normativos e incentivos que permitan generar convergencias entre la información personal y su uso, entre las libertades individuales y el interés público, entre la vida privada y la información pública, entre la interconexión global y las identidades locales, entre la tecnología y la humanidad».

6. Medidas adoptadas por el Estado en materia de ciberseguridad

Como se ha venido anticipando, el Estado de Chile ha ido cumpliendo, paulatinamente, los compromisos que debe adoptar en función de la protección de sus ciudadanas y ciudadanos en el marco de los riesgos a los que se ven expuestos ante el creciente uso de la tecnología en la vida cotidiana de las personas. Particularmente en materia de ciberdelincuencia, atendido el diagnóstico en torno al aumento de los delitos cometidos en el ciberespacio, las medidas son:

- Aprobación del Convenio de Budapest o Convención sobre Ciberdelincuencia del Consejo de Europa, de 2001 y ratificado por Chile en el año 2017.
- Suscripción del protocolo adicional del convenio de Budapest sobre evidencia digital, correspondiente al Segundo Protocolo, suscrito por Chile en 2022.
- Aprobación de la Ley 21.459, publicada y, por ende, vigente desde el 20 de junio de 2022.

- Decreto N° 20, de 20 de diciembre de 2023, del Ministerio de Transportes y Telecomunicaciones que implementa las obligaciones de las empresas de telecomunicaciones sobre preservación provisoria de datos informáticos.

Por otro lado, la actual Ley 21.663, que establece un marco sobre ciberseguridad, ha entrado recientemente en vigencia, con fecha 8 de abril, como se anticipara, dejando pendiente el desafío de su efectiva implementación.

7. Bienes jurídicos protegidos en materia de ciberdelincuencia

Como se señaló, una de las medidas importantes que los Estados deben adoptar para cumplir con sus deberes en ciberseguridad radica en implementar acciones eficaces en el ámbito del derecho penal, es decir, en lo relativo a la ciberdelincuencia.

Y, probablemente, un punto importante sobre el que no existe consenso en materia de delincuencia informática radica en la definición del bien jurídico protegido por esta categoría delictiva, tema que no solo tiene importancia para divagaciones de orden doctrinario, sino también respecto de múltiples aspectos prácticos. En efecto, desde la perspectiva del derecho penal sustantivo, la definición de bien jurídico cumple funciones de gran relevancia entre las que puede mencionarse el hecho de que la afectación de un bien jurídico permite fundamentar el castigo punitivo de las conductas que lo lesionan o ponen en peligro y constituye un requisito ineludible para el ejercicio del *ius puniendi*, y contribuye a sistematizar los tipos penales que conforman la Parte Especial y a comprender la interpretación de los comportamientos que ellos reprimen.[6] Sin embargo, desde la perspectiva instrumental nos encontramos con efectos aún más palmarios de la importancia de la definición, como el hecho de conocer la disponibilidad del bien jurídico protegido y su carácter, para efectos de procedencia de un acuerdo reparatorio, o si aplicaremos normas de reiteración de delitos, conforme al artículo 351 del Código Procesal Penal.

La discusión, a grandes rasgos, se organiza en torno a dos grandes posiciones. En primer lugar, aquella que estima que no existe un bien jurídico especial protegido por esta categoría delictiva, sino que el mismo

6 Mayer (2017), pp. 235-236.

corresponderá al tipo penal de que se trate, vía una especie de extensión del delito «no informático» al que podría asimilarse el delito informático, de forma que la informatización apuntaría más a una modalidad de comisión de distintas figuras penales, antes que a una categoría delictiva propiamente tal. Así, podríamos encontrarnos ante un delito contra la propiedad, la intimidad, la fe pública o la seguridad, dependiendo del tipo penal específico. Por otro lado, la tendencia contraria apunta a encontrar un bien jurídico propio y específico de esta categoría delictiva, sin importar la figura que podría encontrarse a la base, por cuanto se trata de una nueva y diferente necesidad de protección de tipo penal.

Para considerar este tema es preciso efectuar una distinción inicial que consiste en comprender que podemos estar ante cuestiones diferentes cuando hablamos de «delitos informáticos». Así, nos dice Mayer que, en sentido amplio, el concepto de criminalidad informática o criminalidad cometida «mediante» sistemas informáticos, «[…] suele utilizarse para referir la comisión de delitos tradicionales a través de computadoras o de Internet (*v. gr.* extorsión o difusión de pornografía infantil). En cambio, la expresión criminalidad informática en sentido estricto, criminalidad cometida "respecto de" o "contra" sistemas informáticos o, simplemente, criminalidad informática, suele emplearse para aludir a comportamientos delictivos que inciden, directamente, en un sistema informático (*v. gr.* sabotaje o espionaje informático). Por su parte, el concepto de "cibercrimen" suele utilizarse para aludir a la criminalidad informática (en sentido amplio o estricto) llevada a cabo a través de Internet. Ahora bien, de acuerdo con la doctrina, no toda conducta (delictiva) que recae en un sistema de tratamiento automatizado de información constituye un delito informático en estricto sentido. Por el contrario, ha de tratarse de comportamientos que incidan en el *software* o soporte lógico, esto es, en los programas, instrucciones y reglas informáticas que permiten el procesamiento de datos en una computadora. A diferencia de ellos, las conductas que solo afectan el *hardware* o soporte físico de un sistema informático, o sea, los componentes que integran la parte material o tangible de una computadora, pueden ser subsumidas, en términos generales, en los delitos (patrimoniales) clásicos y, muy especialmente, en el tipo penal de daños».[7]

7 Mayer (2017), pp. 237.

Es importante consignar que hay elementos de interpretación fundados en la historia de la ley que permiten orientarnos en la materia. En efecto, la Ley 19.223, antecedente directo de la Ley 21.459 en cuanto tratamiento de carácter penal de los llamados «delitos informáticos», declaraba expresamente en la moción que le daba origen que su articulado tendía a la tutela de un nuevo bien jurídico, correspondiente a «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 obtienen». De este modo, hace treinta años el legislador consideraba que debía apuntarse hacia un bien jurídico específico, propio de esta emergente criminalidad. Por el contrario, el mensaje de la Ley 21.459, en el lado opuesto, plantea que «[...] 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 delitos, 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» (énfasis añadido).[8]

Si bien en caso alguno pretendemos restarle importancia al tema, sí nos parece imprescindible detenernos en la vertiginosidad de la cuestión, lo que torna a lo menos difícil la posibilidad de llegar a conclusiones categóricas. En efecto, la velocidad de los avances en sede de tecnologías de la información nos llama a estar en permanente actualización y a revisar constantemente las definiciones que se pueden adoptar.

Y, además de esta característica tan patente cuando hablamos de avances tecnológicos, debemos también considerar la interconexión con otros fenómenos con los que esta materia, claramente de orden transversal, se va relacionando y que pueden ir determinando sus consecuencias. En tal sentido, cabe considerar la reciente Ley de Delitos Económicos, contenida en la Ley 21.595, vigente desde el 17 de agosto de 2023,[9] cuyo artículo 2° establece que «Serán, asimismo, considerados como delitos económicos los hechos previstos en las disposiciones legales que a continuación se indican, siempre que el hecho fuere perpetrado en ejercicio de un cargo, función o posición en una empresa, o cuando lo fuere en

8 BCN (2022), s.p.

9 Para personas naturales, sin perjuicio de su vacancia legal para personas jurídicas, respecto de las que entró en vigencia el 1 de septiembre de 2024.

beneficio económico o de otra naturaleza para una empresa: [...] 20. Los artículos 1°, 2°, 3°, 4°, 5°, 6°, 7° y 8° de la Ley 21.459, que establece normas sobre delitos informáticos, deroga la Ley 19.223 y modifica otros cuerpos legales, con el objeto de adecuarlos al Convenio de Budapest».[10]

Vale decir, todos los delitos informáticos que contempla la Ley 21.459, cada vez que se dé el supuesto de contexto corporativo, esto es, que el hecho haya sido perpetrado en ejercicio de un cargo, función o posición en una empresa, o cuando lo hubiere sido en beneficio económico o de otra naturaleza para una empresa, corresponderán a delitos económicos, con el importante catálogo de consecuencias que dicha normativa contempla, partiendo por un régimen especial para la determinación de penas, con circunstancias modificatorias de responsabilidad penal especiales, la exclusión de ciertas penas sustitutivas de la Ley 18.216 y la aplicación de un sistema de sanciones pecuniarias totalmente distinto –sistema de días-multa–, que operaría ante la comisión de estas figuras penales.

En este escenario, nos parece que cualquier definición que se adopte en esta materia deberá depender del delito específico de que se trate, siendo conveniente, por ahora, hacer planteamientos más amplios, que contribuyan a la mejor solución para cada caso.

8. Marco internacional en materia de ciberdelincuencia

En esta sección revisaremos los principales aspectos internacionales que regulan la materia.

8.1. Convenio de Budapest

El Convenio de Budapest sobre Ciberdelincuencia es un tratado internacional abierto a firma en el año 2001 e impulsado por el Consejo de Europa con el objetivo de incrementar la cooperación internacional y generar marcos legales armónicos entre las naciones para hacer frente a los delitos informáticos y a la actividad criminal en Internet.

Con más de veinte años de existencia, además de haber sido el primer tratado internacional en la materia, se considera la norma internacional

10 Cabe también tener presente la consideración como delito económico en el mismo artículo 20, en el numeral 7: «El artículo 7, letras f) y h), de la ley Nº 20.009, que Establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude».

más completa hasta la fecha, ya que proporciona un marco integral y coherente sobre el ciberdelito y la evidencia electrónica. Sirve como una guía para cualquier país que desee desarrollar una legislación nacional integral sobre ciberdelitos y como un marco para la cooperación internacional entre los Estados parte de este tratado. De esta forma, sigue constituyendo uno de los principales textos legales sobre cooperación internacional con fines de persecución penal y lucha contra el ciberdelito. Argentina, Chile, Costa Rica, Colombia, Panamá, Paraguay, Perú y República Dominicana son los países latinoamericanos que han suscrito el Convenio, mientras que Ecuador, Guatemala, México y Brasil son observadores.

El Convenio está compuesto de dos secciones, una primera referida a derecho penal sustantivo, que contempla criminalización de conductas que van desde el acceso ilícito, ataques a la integridad del sistema y de los datos hasta el fraude informático y los delitos relacionados con la pornografía infantil, y una segunda parte, que se aboca a las cuestiones de derecho procesal, como ciertas herramientas que permitan hacer más efectiva la investigación relacionada con ciberdelitos y la obtención de evidencias electrónicas, así como a temas de jurisdicción y cooperación internacional.

Chile ratificó este convenio con fecha 20 de abril de 2017 y entró en vigencia para nuestro país el 1 de agosto de ese mismo año.

Uno de los principales objetivos del Convenio de Budapest es mejorar las condiciones de los países miembros para actuar coordinadamente en el combate contra la cibercriminalidad, por lo que es crucial realizar esfuerzos que permitan la armonización del Convenio con las legislaciones locales.

En el proceso de ratificación del Convenio de Budapest, Chile planteó algunas reservas. En primer lugar, sobre el artículo 4° de la convención, respecto de los ataques a la integridad de los datos, por cuanto el Convenio alude a conductas que «comporten daños graves», lo cual constituye un concepto muy indefinido, que amenaza el principio de taxatividad del derecho penal.

Una segunda reserva se realizó sobre el artículo 6° párrafo uno de la convención, referente al abuso de dispositivos. En concreto, la reserva señala que no se tipificará el abuso de los dispositivos «en la medida que ello no afecte la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del citado artículo 6».

También hubo reserva sobre el artículo 29 de la convención, relativo a la conservación rápida de datos informáticos y de acuerdo con el cual otro país podría exigirle a Chile conservar datos necesarios para una investigación criminal. La reserva tiene como fundamento respetar el principio de doble tipicidad penal; es decir, el país podría negarse a conservar datos si es que el delito que se investiga en el extranjero no constituyese delito en Chile.[11]

8.2. Primer Protocolo Adicional al Convenio sobre Ciberdelincuencia del Consejo de Europa

Este protocolo fue suscrito en la ciudad de Estrasburgo, con fecha 28 de enero de 2003, y tiene por objeto la lucha contra el racismo, la discriminación racial, la xenofobia y la intolerancia, en el ámbito de los sistemas informáticos –y, en particular, a través de Internet–, penalizando jurídicamente los actos racistas y xenófobos. El objetivo del Protocolo es la asistencia mutua en la armonización de la legislación penal sustantiva, en cuanto a la lucha contra el racismo y la xenofobia en la web, así como mejorar la cooperación internacional en esta área. A nivel nacional, las partes firmantes deberán tomar medidas legislativas, o de otra índole, para evitar la difusión de material racista y xenófobo mediante sistemas informáticos; impedir que mediante las redes se emitan amenazas o insultos con motivación racista o xenófoba; y también prevenir cualquier uso de sistemas informáticos para negar o justificar genocidios o crímenes contra la humanidad.

Chile, que solo es parte del Convenio desde el año 2017, no suscribió el Primer Protocolo Adicional.

8.3. Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia del Consejo de Europa.

El segundo Protocolo del Convenio de Budapest ha tenido en cuenta la proliferación del delito cibernético y la creciente complejidad de obtener pruebas electrónicas que pueden almacenarse en jurisdicciones extranjeras, múltiples, cambiantes o desconocidas, y el hecho de que los poderes de las fuerzas del orden están limitados por las fronteras territoriales.

11 Becker y Violier (2020), P. 80.

Por ello, este Segundo Protocolo se ha centrado en todos los aspectos prácticos derivados de la complejidad en el esclarecimiento de este tipo de delitos y la urgente necesidad de avanzar en esa línea, para que todos los esfuerzos en materia de tipificación no pierdan sentido ante las propias circunstancias de la delincuencia informática, caracterizada, entre otros aspectos, por la ausencia de fronteras, con los consiguientes problemas jurisdiccionales y relativos a la obtención, mantención, custodia, transporte, etc., de evidencia digital y prueba electrónica idónea para responder a un fenómeno cambiante y creciente. El Segundo Protocolo argumenta que es necesario abordar la situación para que los sistemas punitivos no caigan en el descrédito tras fracasar en un ámbito transversal para las sociedades actuales. Consideraremos en mayor profundidad este punto en el capítulo final.

8.4. Modelo de cooperación internacional

La cooperación internacional pasa a constituirse en uno de los supuestos fundamentales que contempla la ciberdelincuencia, lo que resulta evidente cuando pensamos en cuestiones tan lógicas como el principio de ejecución del delito de que se trate o el lugar donde se encuentra la evidencia digital. En definitiva, la transnacionalización se erige como una cuestión central en la normativa sobre cibercriminalidad y el objetivo apunta a regular de la manera más eficiente casos en los que las conductas tengan lugar en un país, la víctima de encuentre en otro, el sistema afectado en uno distinto y lo mismo ocurra con los antecedentes necesarios para el esclarecimiento de los hechos. Todos estos supuestos están regidos por distintas legislaciones, todas ellas conscientes de la importancia de evitar la impunidad de los hechos.

Eso es lo que resulta recogido por el Convenio de Budapest. En efecto, el Capítulo III de la convención alude a la cooperación internacional, regulando temas como la extradición, la preservación de los datos, el acceso fronterizo de datos, la Red 24/7 establecida en el artículo 35 para fines de asesoría, y la preservación y obtención de ciertos datos, y concluye con las solicitudes de asistencia internacional por vías formales (*mutual legal assistance*).

Capítulo 2

Aspectos sustantivos en la legislación sobre ciberdelincuencia

1. Injusto informático

Como se anticipó, existe en la doctrina nacional e internacional una discusión sobre cuáles son los bienes jurídicos protegidos por los delitos informáticos, y se identifican dos posturas principales. Por un lado, una postula que los delitos informáticos serían tan solo nuevas modalidades delictivas para cometer delitos ya conocidos por nuestra legislación, tales como la estafa, la violación de secreto, la difusión de pornografía infantil, entre otros. En este sentido, los bienes jurídicos protegidos por estos nuevos tipos penales serían los mismos que protegen las figuras típicas clásicas.

Otra postura plantea, en cambio, que existiría un bien jurídico nuevo, propiamente informático, y que consiste en «la integridad, confidencialidad y disponibilidad de los sistemas informáticos, y de los datos contenidos en ellos».[12] Esta segunda posición doctrinal se funda en la creciente importancia que han adquirido y revisten los procesos de transmisión y tratamiento de datos informáticos, transformándose estos últimos en una plataforma vital para el desarrollo de intereses individuales y para el mantenimiento de objetivos macrosociales e institucionales, tales como la seguridad nacional, la estructura de servicios masivos y la economía.[13]

Por otra parte, un análisis de la Ley 21.459 a la luz del Convenio de Budapest, promulgado a través del Decreto Supremo 83/2017 del Ministerio de Relaciones Exteriores, y que constituye el esfuerzo regulatorio más relevante en la unificación de las tipologías delictivas asociadas a la realidad informática, nos permite observar que los delitos contemplados en esta ley constituyen en su mayoría delitos informáticos *stricto sensu*, es decir, aquellos cometidos respecto o *contra* sistemas informáticos,

12 Bascur y Peña (2022), p. 4.
13 *Ídem.*

tales como el sabotaje informático, en contraposición a aquellos delitos que se cometen *mediante* sistemas informáticos, como, por ejemplo, una extorsión ejercida a través de una página web.[14] Debe también precisarse que no toda conducta delictiva que recae en un sistema de tratamiento automatizado de información constituye un delito informático en sentido estricto,[15] ya que para esto ha de tratarse de comportamientos que incidan en el *software* o soporte lógico, es decir, en los programas y reglas informáticas que permiten el procesamiento de datos en una computadora,[16] quedando excluidas aquellas conductas que solo afecten el *hardware* o soporte físico de un sistema informático.

Lo mencionado anteriormente es relevante únicamente respecto de los primeros, es decir, de los delitos informáticos *stricto sensu*, donde tiene sentido la discusión respecto de la existencia o no de un bien jurídico propiamente informático. Un importante sector de la doctrina considera que las conductas que tienen como objeto de ataque los componentes lógicos de un sistema informático, tanto los datos específicamente considerados como el funcionamiento de un sistema concreto, y cuya ejecución incide perjudicialmente sobre alguna de sus tres condiciones básicas de operación: integridad, confidencialidad y disponibilidad de datos, o un sistema, serían conductas expresivas del menoscabo de un bien jurídico de carácter colectivo o supraindividual, en tanto las propiedades de los sistemas informáticos ya mencionadas (integridad, confidencialidad y disponibilidad) representan, individual o conjuntamente consideradas, un contenido de antijuridicidad autónomo.[17]

Clásicamente se ha considerado que existen tres formas comisivas principales de los delitos informáticos; por un lado, aquellas que implican destrucción o inutilización de datos o programas de sistemas informáticos, englobadas en la categoría de sabotaje informático, y que afectarían la integridad de los datos o el sistema; por otro lado, las que suponen acceso u obtención indebida de datos o programas informáticos, denominadas genéricamente como espionaje informático y que afectarían la confidencialidad de los datos o el sistema, y por último, las conductas que implican alteración o manipulación de datos o de siste-

14 Mayer (2017), p. 237.
15 *Ídem.*
16 *Ídem.*
17 Bascur y Peña (2022), p. 5.

mas informáticos, relacionadas con el llamado fraude informático, que lesionarían la disponibilidad de los datos o del sistema informático en su conjunto.[18] Aunque esta trilogía de bienes jurídicos ha sido criticada por cierta doctrina,[19] que sostiene que lo realmente protegido es la funcionalidad informática, concepto que abarcaría el desenvolvimiento o funcionalidad regular de los procesos automatizados sobre datos que ejecutan los sistemas informáticos, de todas formas es una herramienta útil para sistematizar los tipos penales contemplados en la nueva Ley 21.459.

Por último, otro sector de la doctrina estima que los delitos informáticos constituyen figuras delictuales pluriofensivas, es decir, que afectarían más de un bien jurídico.[20] En este sentido, podríamos señalar que el bien jurídico protegido en general sería la información, pero que esta es considerada de distintas formas, ya sea como un valor económico o un valor intrínseco de la persona, por su fluidez y tráfico jurídico, y por los sistemas que la procesan o automatizan.[21] Siguiendo esta misma línea de razonamiento, los bienes jurídicos tradicionales que se ven afectados por los delitos informáticos serían el patrimonio, en el caso de los fraudes informáticos y la manipulación de datos; la reserva, intimidad y confidencialidad de los datos, en el caso de los ataques informáticos a la esfera de la intimidad en general; y la seguridad y fiabilidad del tráfico jurídico y probatorio, en el caso de la falsificación de datos.[22]

Como se adelantó, esta última tesis sobre los bienes jurídicos protegidos por los delitos informáticos parece ser aquella considerada por los redactores del proyecto de la Ley 21.459,[23] que vino a derogar a la antigua Ley 19.223, ya que en el mensaje presidencial que dio origen a la tramitación parlamentaria del proyecto de ley se plantea que «[…] 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 delitos, mantenerlo como una ley de carácter especial, en atención a los múltiples bienes jurídicos protegidos, no solo la integridad o confiabilidad de la información contenidas en sistemas de información».[24]

18 Arenas (2022), p. 31.
19 Mayer y Oliver (2020), p.153.
20 Arenas (2022), p. 32.
21 Acuario (2016), p. 20.
22 Arenas (2022), p. 32.
23 *Ídem.*
24 BCN (2022), s.p.

2. Tipos penales contemplados en la Ley 21.459

A continuación, se realizará un análisis dogmático de los distintos tipos penales contemplados en la Ley 21.459, utilizando como criterio para categorizarlos la clasificación ya enunciada anteriormente, que distingue entre aquellas conductas delictivas que afectan la integridad de los datos o de los sistemas informáticos, conductas denominadas *sabotaje informático*, que se encuentran reguladas principalmente en los artículos 1° y 4° de la mentada ley; las conductas delictivas que atacan la confidencialidad de los datos y sistemas, denominadas *espionaje informático*, y finalmente aquellas conductas que alteran o modifican el contenido de los datos o sistemas, afectando su disponibilidad, y que se engloban en la categoría de *fraude informático*.

Para efectos de una mayor claridad conceptual, es importante mencionar que la Ley 21.459 (o LDI) se encarga de definir los conceptos de datos informáticos y sistema informático, y es en este sentido en el que serán utilizados. El artículo 15 letra a) define datos informáticos como «Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función». Vale decir, se comprenden como unidades básicas de información bajo la forma de impulsos electromagnéticos procesados.[25] Por otra parte, no se contemplan efectos jurídicos especiales si los datos objeto de la conducta delictiva constituyen «datos personales», de acuerdo con lo establecido en la Ley 19.628, no obstante la eventual utilidad que tengan para determinar la cuantía exacta de la pena, en aplicación del artículo 69 del Código Penal.[26]

Por su parte, un sistema informático es definido como «Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de algunos de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa». Es decir, se considera sistema a todo elemento destinado a la creación, envío, recepción, procesamiento y almacenamiento de datos, a partir de secuencias lógicas de instrucciones o indicaciones para la realización de tareas y obtención de resultados informáticos, conforme a las reglas predeterminadas por el usuario titular.[27]

25 Bascur y Peña (2022), p. 6.
26 *Ídem.*
27 *Ídem.*

Vale tener en consideración que existe una figura delictiva en la nueva LDI que no se puede encuadrar en ninguna de las tres categorías de delitos ya mencionadas, y corresponde al abuso de dispositivos, tipificada en el artículo 8° de la ley, que se refiere a hechos relativos a la gestión o intermediación de elementos (como datos informáticos) necesarios para la ejecución de ciertos delitos taxativamente enumerados.[28] Podría considerarse también como una figura autónoma la tipificada en el artículo 6° de la ley, la receptación informática, conducta consistente en actos tanto de disfrute de los efectos de datos provenientes de un catálogo cerrado de delitos informáticos como de preparación.[29]

Por último, existen dos tipos delictivos cuya lesividad es compleja de establecer, que son la falsificación informática y el fraude informático, contemplados en los artículos 7° y 5° de la ley, respectivamente. En estricto rigor, constituyen delitos informáticos en sentido amplio o impropio, ya que son delitos que afectan bienes jurídicos tradicionales, como la seguridad del tráfico jurídico o el patrimonio, y constituyen en el fondo modalidades virtuales de delitos ya contemplados por la legislación penal chilena, pero cuya comisión a través de medios informáticos ha aumentado en los últimos años, razón que justificaría su inclusión en la Ley de Delitos Informáticos. No obstante, también exhiben propiedades de delitos informáticos *stricto sensu,* al comprometer la integridad informática. Ahora, un eventual aspecto problemático al respecto es si estos delitos constituyen o no figuras de lesión o de peligro abstracto en contra del bien jurídico informático, situación no menor en tanto determinaría la aplicación, o no, de reglas especiales de determinación de la pena que le asignan al bien jurídico una función dogmático-interpretativa, como sería el caso del artículo 351 del Código Procesal Penal, con la figura de la reiteración de delitos.[30]

Nosotras consideramos que, por razones sistemáticas, debido a su ubicación en la Ley de Delitos Informáticos, y por razones criminológicas, debido a que para cometer estos delitos es necesario afectar de cierta forma la integridad de datos informáticos o un sistema informático, resulta una postura más acertada la de considerarlos como delitos que afectan a la información entendida como un bien jurídico supraindividual o colectivo.

28 *Ídem.*
29 *Ídem.*
30 *Ídem.*

2.1. Sabotaje informático

Como ya se ha venido señalando, la expresión «sabotaje informático» se utiliza, por lo general, para designar conductas de destrucción e inutilización de datos y sistemas informáticos, y se manifiesta en actos de eliminación no autorizada de los mismos.[31]

A) Ataque a la seguridad de un sistema de información (artículo 1°, Ley 21.459)

Se revisará a continuación cada aspecto relevante por separado.

a. conducta típica

El artículo 1° de la Ley 21.459 establece: «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».

De la lectura del tipo penal recién transcrito se observa que el verbo rector denotativo utilizado por el legislador es «obstaculizar o impedir». Más adelante, indica las formas o modalidades en que el sujeto activo puede realizar esta obstaculización o impedimento, siendo estas la «introducción, transmisión, daño, deterioro, alteración, o supresión de los datos informáticos».

Una duda que surge del análisis de la conducta típica de este delito es si exige o no un resultado material que implique el efectivo menoscabo a la integridad de los datos o del sistema informático atacado, en especial si lo comparamos con el artículo 4° de la misma ley, que exige para la configuración del delito de ataque a la integridad de los datos un daño grave al titular de los mismos. La respuesta que parece más lógica y coherente es señalar que es necesario que el sujeto activo efectivamente obstaculice o impida el normal funcionamiento del sistema informático, al menos parcialmente, lo que requiere una transformación del mundo externo a través de la conducta, no obstante no ser necesario que por esta acción se cause un daño al titular del sistema informático, si

31 *Ídem.*

lo hubiera.[32] Por otra parte, para cautelar la vigencia del principio de proporcionalidad, es necesario que el impedimento parcial genere una afectación equivalente en cuanto a su gravedad a los casos de impedimento total del sistema informático, debido a que ambas conductas están castigadas con la misma pena.[33]

Respecto a la posibilidad de que sea admisible la comisión por omisión de este o cualquier otro delito contemplado en la Ley de Delitos Informáticos, llama la atención el inciso final del artículo primero transitorio de la Ley 21.459, según el cual, para efectos de lo dispuesto en los incisos primero y segundo de dicho precepto, «el delito se entiende perpetrado en el momento o durante el lapso en el cual se ejecuta la acción punible o se incurre en la *omisión* punible» (énfasis añadido).

Cabe indicar que ninguno de los ocho delitos tipificados en la ley contempla una comisión omisiva expresa, y esta cláusula transitoria podría hacer pensar que habilitaría el castigo de hipótesis de omisión impropia en el ámbito de la criminalidad informática. Sin embargo, esta tesis no es compartida por cierta doctrina por diversos motivos, tales como el hecho de no indicarse los requisitos para el castigo de la omisión impropia, como la concurrencia de una posición de garante; su ubicación como norma transitoria, y la falta de compatibilidad de las conductas descritas en los tipos penales con comisiones omisivas.[34] Es por estas razones que el tipo penal analizado se considera un delito de acción y no podría ser ejecutado mediante conductas omisivas.

B. ITER CRIMINIS

De acuerdo con el sentido expresado en el párrafo anterior, el ataque a la seguridad de un sistema informático es un delito de resultado y, por lo tanto, compatible con modalidades de ejecución imperfecta del delito, como la tentativa y el delito frustrado. Un ejemplo de esto sería que un sujeto empezara a introducir datos falsos a un sistema informático para alterar su funcionamiento, pero sea detenido antes de impedir el funcionamiento debido al actuar de los sistemas de ciberseguridad del sistema en cuestión. También es posible imaginar supuestos de frustración de este delito, como sería el caso de aquel delincuente informático

32 Mayer y Vera (2022b), p. 271.
33 *Ídem.*
34 *Ídem.*

que logra transmitir datos a un sistema informático, con la intención de impedir su funcionamiento, pero debido a causas externas no logra impedir ni siquiera parcialmente el funcionamiento del sistema.

C. RESULTADO MATERIAL

El delito de ataque a la integridad de un sistema informático, como ya se señaló, es un delito de resultado, ya que exige un resultado en el plano fáctico que es la efectiva obstaculización o impedimento de funcionamiento de un sistema informático. Ahora bien, si entendemos esta figura como una forma de sabotaje informático, siendo el sabotaje informático un delito que tiene como fin la protección de la integridad de un sistema informático, la cual, a su vez, se comprende como el mantenimiento de los datos informáticos o del sistema, resulta plausible considerarla como un delito de puesta en peligro, en tanto no se exige una eliminación o inutilización definitiva de los datos o el sistema. La obstaculización o impedimento puede ser parcial y temporal, y el delito se configuraría de cualquier forma, aunque los datos o el sistema no resulten en definitiva eliminados o inutilizados.

D. SUJETO ACTIVO Y PASIVO

El tipo penal no establece ninguna exigencia respecto al sujeto activo del delito, utilizando simplemente la expresión «El que […]». Respecto al sujeto pasivo, al ser este un delito que atenta contra un bien jurídico supraindividual, no existe una víctima determinada del mismo y, por tanto, no es necesario que se configure un daño específico a una persona determinada que opere como víctima del delito.

E. ASPECTO SUBJETIVO

Con relación a la posición anímica del sujeto activo, el tipo penal no incorpora ningún elemento subjetivo propio, como sí lo hacen, por ejemplo, los artículos 2° y 7° de la Ley 21.459, a propósito del acceso ilícito y el fraude informático, tales como el ánimo de lucro o el ánimo de apoderamiento. Tampoco menciona el dolo y, por tanto, es en principio compatible con ejecuciones realizadas con dolo directo y dolo eventual. Esto representa una diferencia respecto de la tipificación que hacía la derogada Ley 19.223, que señalaba que la conducta debía ser ejercida

maliciosamente.[35] Ahora, resulta complejo imaginar supuestos en que la conducta típica pueda ser realizada con dolo eventual, pero su castigo está permitido por la actual legislación.

Por otra parte, la comisión culposa queda descartada por razones lógicas y sistemáticas; en primer lugar, al ser una ley penal especial, se encuentra fuera del Título VIII del Código Penal, lo que trae como consecuencia que no se aplique la cláusula del artículo 492 del mismo código, y a falta de texto expreso que establezca una modalidad culposa aplicable para los delitos informáticos, esta no puede ser castigada.[36] Por otra parte, resulta muy difícil, casi imposible, concebir la realización de un *ataque* a la integridad de un sistema informático por mera imprudencia.

B) Ataque a la integridad de los datos (artículo 4°, Ley 21.459)

Se revisará por separado cada uno de los aspectos relevantes sobre este tema.

a. conducta típica

El artículo 4° de la LDI reza: «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». Este delito tiene su antecedente directo en el artículo 4° del Convenio de Budapest.[37]

El verbo rector denotativo del tipo penal es «alterar, dañar o suprimir datos informáticos». De acuerdo con la tipología con base en la cual se realiza esta clasificación, sería una combinación entre sabotaje informático, por la expresión «dañar o suprimir», y fraude informático, por la expresión «alterar». Respecto a la posibilidad de castigar un comporta-

35 Artículo 1°: «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».

36 Etcheberry (2010), p. 321.

37 Artículo 4°: «Ataques a la integridad de los datos.
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves».

miento omisivo como modalidad ejecutiva de este delito, nos remitimos a lo ya señalado con relación al delito de ataque a la integridad de un sistema informático.

B. ITER CRIMINIS

Existe discusión en la doctrina respecto a si este delito constituye un delito de resultado o no, debido a la expresión «siempre que con ello se cause un daño grave al titular de estos mismos». Para algunos, el daño grave al titular de los datos correspondería al resultado material del delito y, en consecuencia, esta figura típica sería compatible con las figuras de tentativa y frustración. Esto se sustenta en que el tipo exige que se *cause* un daño, evocando la relación de causalidad necesaria en todo delito de resultado.[38]

Otra posición doctrinal, no obstante, argumenta que el «daño grave al titular de estos mismos» sería realmente una condición objetiva de punibilidad, debido a que el tipo penal parece supeditar el castigo de la conducta a la verificación de una circunstancia, que sería el daño grave, además de que la redacción es similar a la de otras figuras penales, las cuales han sido interpretadas como condiciones objetivas de punibilidad. Este es el caso, por ejemplo, del abandono de personas desvalidas del artículo 352 del Código Penal, de acuerdo con el cual «[e]l que abandonare a su cónyuge o a un ascendiente o descendiente, legítimo o ilegítimo, enfermo o imposibilitado, si el abandonado sufriere lesiones graves o muriere a consecuencia del abandono, será castigado con presidio mayor en su grado mínimo».

Parece ser que esta segunda postura es más compatible con el tenor de la discusión parlamentaria de la ley, en la cual se dejó constancia de la necesidad de evitar el castigo de este delito cuando no tuviera un impacto relevante en intereses de terceros,[39] en coherencia también con lo señalado en el artículo 4° número 2 del Convenio de Budapest.[40] Así, este sería un delito de mera actividad respecto del cual no cabría el castigo de modalidades imperfectas de ejecución (tentativa, delito frustrado).

38 Mayer y Vera (2022b), p. 276.
39 BCN (2022), pp. 111 y 112.
40 Mayer y Vera (2022b), p. 277.

C. RESULTADO MATERIAL

Como ya se señaló en el apartado anterior, existe discusión respecto a si el delito de ataque a la integridad de los datos es un delito de resultado o de mera actividad, pero hay acuerdo en que es un delito de lesión, ya que se requiere una efectiva afectación al titular de los datos alterados, dañados o suprimidos. Cabe indicar que la ley no especifica qué tipo de daño se exige para la configuración del delito, solo señala que debe ser «grave», expresión ambigua, que otorga una amplia discreción al tribunal. La gravedad del daño es algo que deberá ser evaluado por el juez caso a caso; no obstante, se ha planteado como un criterio orientador de la actividad jurisdiccional la mayor o menor complejidad para recuperar los datos informáticos afectados por la conducta delictiva.[41-42]

41 Mayer y Vera (2022b), p. 276.

42 La alusión a la gravedad también se contempla en la legislación española, conforme a la reserva que permite el Convenio de Budapest en su artículo 4°. El Tribunal Supremo Español analizó este punto en el caso del STS 528/2022, en el cual se le reprochaba a la imputada haber ingresado al sistema informático de su empleador para eliminar todos los datos de los clientes tras su desvinculación.

El máximo tribunal español señaló que «la gravedad del resultado debe apreciarse en el caso enjuiciado, pues 'fueron borrados los archivos informáticos que contenían toda la información de las ventas, productos y clientes de la zona de Portugal, archivos que pertenecían a la mercantil Escribano Levante S.L. y que resultaban determinante[s] para el ejercicio de su labor comercial en dicha zona, no habiendo podido ser recuperada la información al haber efectuado la acusada un borrado total o seguro que lo hace irreversible, y no existir copias de seguridad'. Y añade también 'No habiéndose podido recuperar los datos borrados por la acusada, propiedad de la empresa, y no existiendo copia de seguridad de los mismos, se concluye la gravedad del resultado perjudicial ocasionado a la mercantil Escribano Levante S. L. por la acusada, más aún cuando se trata de una empresa de ventas por teleoperadores habiéndose producido un borrado de los datos de los clientes correspondientes a la zona de Portugal, zona de la que estaba a cargo la acusada, afirmando la testigo Camila, directora comercial de Escribano Levante S.L., que se vieron obligados a llevar a cabo un nuevo estudio de mercado de la zona de Portugal con el correspondiente retraso en el comercio y venta de sus productos y pérdida de clientes. *La gravedad de los resultados, con un barrido casi total de la información correspondiente a las ventas y clientes de la zona de Portugal, y la deliberada intencionalidad de la acusada en la producción de dichos daños, determinan la calificación de su acción como grave*'» (énfasis añadido).

D. SUJETO ACTIVO Y PASIVO

Con relación al sujeto activo, el tipo agrega la palabra «indebidamente» a continuación de «El que»; por tanto, es necesario que la persona que ejecute la conducta típica no cuente con autorización para realizarla, como sería el caso de que el titular del sistema informático y de los datos contenidos en él le solicite al encargado de informática de la entidad en que ambos prestan servicios que borre información almacenada en dicho sistema.[43] En este caso, el consentimiento del titular del sistema o de los datos operará como causal de atipicidad.

E. ASPECTO SUBJETIVO

En el ámbito subjetivo, el tipo penal no contempla requisito subjetivo alguno que apunte, necesariamente, a exigir dolo directo (*v. gr.*, una actuación «a sabiendas»), por lo que basta con que el delito se perpetre mediante dolo eventual. La modalidad culposa debe ser descartada, por las mismas razones señaladas a propósito del ataque a la integridad de un sistema informático.[44]

2.2. Espionaje informático

La segunda categoría en la cual clasificaremos a los delitos informáticos corresponde a la del espionaje informático. Se comprenden dentro de esta categoría aquellos atentados contra la confidencialidad de los sistemas o datos informáticos, actos que violentan la *expectativa de exclusión* que ostenta el usuario-titular de un sistema en la gestión de los datos almacenados en su interior, y se protege la restricción o limitación de acceso y conocimiento de estos frente a terceros,[45] siendo este en definitiva el bien jurídico protegido por esta clase de delitos, como lo es la integridad del sistema o los datos en los supuestos de sabotaje informático.

Los delitos de la LDI que pertenecen a esta categoría son los siguientes: a) el acceso ilícito, tipificado en el artículo 2° inciso primero; b) espionaje informático, previsto en el inciso segundo del artículo 2° como una figura calificada de acceso ilícito; c) divulgación de datos obtenidos

43 Mayer y Vera (2022b), p. 276.
44 *Ídem.*
45 Bascur y Peña (2022), p.4.

ilegalmente, figura contemplada en el inciso tercero del artículo 2°, y d) interceptación ilícita, regulada en el artículo 3° de la ley.

Por motivos técnico-jurídicos, en el siguiente acápite analizaremos conjuntamente las figuras de acceso ilícito, espionaje informático y divulgación de datos obtenidos ilegalmente, puesto que estas tres figuras están reguladas en el mismo artículo y tienen como base la misma conducta típica, esto es, el que, sin autorización o excediendo la autorización que posee y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático.

A) Acceso ilícito (artículo 2°, Ley 21.459)

Se revisará cada aspecto relevante por separado.

a. conducta típica

El artículo 2° inciso primero de la Ley 21.459 establece: «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 11 a 20 unidades tributarias mensuales». Esta figura encuentra su antecedente en la derogada Ley 19.223, que, también en su artículo segundo, consagraba: «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» (énfasis añadido). Como se analizará más adelante, la conducta típica recién citada se relaciona más bien con el delito de espionaje informático propiamente tal, consagrado en el artículo 2° inciso segundo de la vigente Ley de Delitos Informáticos, en especial por la exigencia de que exista un ánimo de apoderarse por parte del sujeto activo.

Lo primero que es importante destacar es que el delito de acceso ilícito castiga la simple entrada o penetración en un sistema protegido sin autorización, con prescindencia de la obtención o la intención de obtener los datos ahí almacenados.[46] Estos elementos típicos solo son exigidos para el castigo del espionaje informático, consagrado en el inciso segundo del mismo artículo, que dispone: «Si el acceso fuere reali-

46 *Ídem.*

zado 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». Esto marca la principal diferencia con la tipificación que realizaba la Ley 19.223, que exigía un ánimo de apoderamiento o de uso para la sanción tanto del espionaje informático como del acceso ilícito; la actual legislación solo lo exige respecto del primero.

El tipo está constituido por tres elementos copulativos: la conducta consistente en *acceder* a un sistema informático, que a su vez opera como objeto del delito; que esta conducta se realice mediante la superación de *barreras técnicas* o *medidas tecnológicas de seguridad*; y que la acción se ejecute sin la autorización del titular o excediendo la que este haya dado.[47]

El verbo rector denotativo del tipo es «acceder», que consiste en entrar, penetrar, o ingresar a un sistema ajeno por cualquier método, siendo asimilable a una violación de morada electrónica.[48] Por otra parte, es importante destacar que el objeto de la conducta es un sistema informático en sí considerado y no específicamente los datos que éste contiene, lo cual permite castigar, por ejemplo, la vulneración de la seguridad de un sistema para la subida de ciertos datos al mismo, incluso sin haber accedido a los datos previamente almacenados.[49]

Ahora bien, no basta cualquier acceso para satisfacer las exigencias del tipo penal, ya que es necesario que este acceso se realice superando barreras técnicas o medidas tecnológicas de seguridad, circunstancia que serviría para dar cuenta del interés del titular en mantener el secreto, o libertad de exclusión, sobre sus datos,[50] relacionando por tanto la conducta típica con el bien jurídico protegido, que no es otro que la legítima expectativa de exclusión de terceros. Los mecanismos señalados consisten en toda condición de acceso dispuesta para restringir o limitar la posibilidad de ingreso, contemplando tanto hipótesis delictivas de vulneración de sistemas de seguridad, como un antivirus, y el simple acceso con la clave o contraseña del titular obtenida ilícitamente.[51] Esta exigencia típica corresponde a una opción del Estado de Chile de restringir la tipificación de la conducta de acceso prevista en el artículo 2°

47 *Ídem.*
48 *Ídem.*
49 *Ídem.*
50 *Ídem.*
51 *Ídem.*

del Convenio de Budapest,[52] excluyendo, por tanto, conductas de acceso que no se realicen mediante la superación de algún tipo de barrera o medida de seguridad.

El tercer elemento de la conducta típica, que generó más discusión durante la tramitación parlamentaria de la ley,[53] es la exigencia normativa de que el autor del delito actúe *sin autorización o excediendo la autorización que posea*. La norma señalada debe ser complementada con lo dispuesto en el artículo 16 de la Ley 21.459, que señala: «Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediante la autorización *expresa* del titular del mismo».

El motivo por el cual este elemento objetivo del tipo penal causó una importante discusión parlamentaria fue la toma de posición que esta exigencia representa por parte del legislador en orden a prohibir el llamado «*hacking* ético», que consiste en aquella labor ejecutada por ciertas personas, por lo general expertos en informática, que ingresan a sistemas informáticos ajenos y evalúan sus niveles de amenaza, informando a su titular acerca de los riesgos advertidos y ofreciéndole posibles soluciones.[54] En consecuencia, por la forma en que quedó redactada la actual legislación, el experto informático deberá contar con la autorización expresa del titular del sistema para acceder a él, independiente de su motivación, tal como lo establece el artículo 16 de la Ley 21.459.

Existen en doctrina dos posibles interpretaciones sobre la naturaleza jurídica de esta autorización: mientras algunos indican que sería una causal de justificación, excluyendo por tanto la antijuridicidad de la conducta, otros señalan, en cambio, que sería más bien una causal de atipicidad, al ser la falta de consentimiento del titular del sistema informático un elemento expreso del tipo penal, en el mismo sentido de

52 Artículo 2°: «Acceso Ilícito: Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático».

53 Mayer y Vera (2022b), p. 278.

54 Mayer y Vera (2022b), p. 279.

otros tipos penales de la parte especial del Código Penal, como la violación de morada o el hurto.[55]

Respecto a la posibilidad de que la conducta de «acceder» pueda ser ejecutada de forma omisiva, esta debe ser descartada, por los mismos argumentos que se aportaron a propósito del sabotaje informático. Esto es, que a pesar de que el inciso final del artículo primero transitorio de la ley pareciera abrir una puerta para el castigo de hipótesis de comisión por omisión de estos delitos, la conducta descrita por el tipo penal no es compatible con una ejecución omisiva y, en consecuencia, esta debería ser desechada.

Por último, todo lo señalado con relación a la conducta del acceso ilícito es aplicable también a la figura del espionaje informático, ya que las diferencias entre ambos ilícitos se presentan fundamentalmente en el plano subjetivo. Respecto al delito de divulgación de datos obtenidos ilegalmente, la conducta típica consiste en «divulgar», que, de acuerdo con un sector de la doctrina,[56] consistiría en dar a conocer a terceros la información contenida en el sistema informático. Desde un punto de vista penológico, este delito tiene asignada la misma pena que le corresponde a quien acceda a un sistema informático, sin autorización y superando barreras de protección, con el ánimo de apoderarse o usar la información contenida en el sistema, es decir, el espionaje informático. Ahora, si la persona que realiza la divulgación es la misma que realizó el espionaje, la pena será mayor, esto es, de presidio menor en sus grados medio a máximo.

B. ITER CRIMINIS

En lo que respecta a la estructura del tipo de acceso ilícito, es posible sostener que las cuatro hipótesis alternativas que este regula constituyen delitos de mera actividad, pues basta con que se acceda ilícitamente a un sistema informático, o bien con que se obtenga y/o divulgue la información a la que se ha accedido, para que se configure el tipo penal. Por lo tanto, debe excluirse el castigo de la frustración. En cambio, considerando que dichas modalidades son fraccionables, es posible afirmar que cabe la sanción penal de la tentativa.[57]

55 Mayer y Vera (2022b), p. 283.
56 Mayer y Vera (2022b), p. 285.
57 Mayer y Vera (2022b), p. 283.

C. RELACIONES CONCURSALES

Consideramos relevante hacer una breve mención a los posibles concursos que puedan darse entre el delito previsto en el artículo 2° de la Ley 21.459 y otros delitos cibernéticos, al ser el acceso ilícito a un sistema informático el paso previo para la eventual ejecución de otros ilícitos informáticos. Si el delito relacionado con el acceso ilícito es otro delito informático en sentido estricto, existiría un concurso aparente de leyes penales y, en consideración a la pena y al injusto contenido en esta figura, consideramos que debería quedar absorbido por aquel delito con que se encuentre en relación concursal. Si, en cambio, es un delito informático impropio, que afecte bienes jurídicos distintos de aquel propiamente informático, se aplicarían las reglas de los concurso real o ideal, dependiendo del caso concreto.

D. SUJETO ACTIVO Y PASIVO

Respecto a este punto, la ley no realiza exigencias sobre el sujeto activo, más allá de que debe ser alguien que no cuente con la autorización del titular del sistema informático para acceder a este. Con relación al sujeto pasivo, el delito, como ya se ha dicho, protege una legítima expectativa de privacidad por parte del titular del sistema informático, siendo por tanto un bien jurídico individual del titular del sistema, quien, estimamos, sería la víctima del delito.

E. ASPECTO SUBJETIVO

Desde el punto de vista del dolo, la norma no establece ninguna exigencia; por lo tanto, cabe concluir que cabría la comisión con dolo directo y eventual. La comisión culposa no tendría cabida por las mismas razones lógicas y sistemáticas enunciadas a propósito del sabotaje informático.

Por otro lado, y como ya ha sido anunciado *supra,* la ley exige un elemento subjetivo propio respecto de los delitos de espionaje informático y de divulgación de datos obtenidos indebidamente, consistente en el ánimo de uso o apropiación de los datos contenidos en el sistema al cual se accedió. Este ánimo no se exige respecto del mero acceso ilícito, lo cual representa una diferencia con la forma en la cual se encontraba regulada esta figura en la antigua Ley 19.223.

Sin perjuicio de lo ya señalado, la Ley 21.663, ya referida como Ley Marco de Ciberseguridad, contempla en su artículo 55 un nuevo inciso final del artículo número 2, en los siguientes términos:

> No será objeto de sanción penal por haber incurrido en los hechos tipificados en el inciso primero, el que habiendo accedido a un sistema informático cuyo responsable tenga domicilio en Chile, lo hiciera cumpliendo con las siguientes condiciones:
> 1. Que se encuentre inscrito en el registro que al efecto lleve la Agencia Nacional de Ciberseguridad.
> 2. Que el acceso se haya realizado habiendo informado previamente de ello a la Agencia.
> 3. Que el acceso y las vulnerabilidades de seguridad detectadas hayan sido reportadas al responsable del sistema informático y a la Agencia, tan pronto se hubiere realizado.
> 4. Que el acceso no haya sido realizado con el ánimo de apoderarse o de usar la información contenida en el sistema informático, ni con intención fraudulenta. Tampoco podrá haber actuado más allá de lo que era necesario para comprobar la existencia de una vulnerabilidad, ni habrá utilizado métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de datos.
> 5. Que no haya divulgado públicamente la información relativa a la potencial vulnerabilidad.
> 6. Que se trate de un acceso a un sistema informático de los organismos de la Administración del Estado. En el resto de los casos, requerirá del consentimiento del responsable del sistema informático.
> 7. Que haya dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia.

No obstante ser esta una ley que tiene una vacancia legal de un año, en nuestra opinión aquí es posible identificar verdaderas causales de justificación que tornan lícita la ejecución de conductas subsumibles dentro del tipo penal de acceso ilícito. Correspondería a una causal de justificación equivalente al ejercicio de un cargo, profesión u oficio, cumpliendo además con las condiciones que establece la misma ley. Los numerales 2 a 7 no son sino los requisitos legales para que opere la causal de justificación. En consecuencia, no se puede castigar a los partícipes, ya que la conducta se torna lícita.

Debido a lo reciente de la ley, no existe una abundante jurisprudencia respecto de este delito. Sin embargo, el Tribunal de Juicio Oral en lo Penal de Rancagua dictó sentencia absolutoria en causa RUC 1901349868-K, de fecha 3 de febrero de 2023 por el *delito de acceso ilícito* en los siguientes términos:

> Considerando décimo cuarto: no se rindió probanza alguna destinada a acreditar que los acusados vulnerando el sistema de seguridad del banco o las medidas de seguridad de la víctima fueron quienes realizaron las transacciones reclamadas. No se pesquisó la huella informática de la transacción para determinar cómo se realizó, de qué manera se vulneró el sistema, desde qué computador o lugar geográfico se realizó esta operación ilícita. En definitiva, no existió absolutamente ninguna actividad probatoria por parte del ente persecutor en torno a acreditar de algún modo pericial o técnico informático que fueron los acusados quienes realizaron algún acto (como interceptar, interferir o acceder) que les haya permitido acceder a la cuenta de la víctima y realizar transacciones sin su consentimiento y depositar dinero en cuentas que se encontraban a sus nombres, apropiándose de estos.
>
> […] es un hecho incontrovertible que la norma contenida en el artículo 2° de la Ley 19.223 por la cual se presentó acusación se encuentra actualmente derogada desde el 20 de junio de 2022 por la dictación de la Ley 21.459, no haciéndose cargo de este punto el Ministerio Público pese a ser levantado por la defensa en su alegato de apertura.
>
> [...] ante la inexplicable falta probatoria pericial informática no se puede establecer que los acusados hayan tenido relación con la sustracción de los dineros.

Si bien la absolución tiene que ver fuertemente con un tema probatorio, también existe un principio de pronunciamiento, por parte del tribunal, respecto de la transición en la tipicidad de la conducta, de la cual tampoco se hace cargo, pero sí reprocha al persecutor que no haya justificado su pretensión punitiva en este punto.

B) Interceptación ilícita (artículo 3°, Ley 21.459)

Se revisará cada aspecto relevante de esta figura por separado.

a. conducta típica

El delito de interceptación ilícita se encuentra consagrado en el artículo 3° de la LDI, que reza:

> 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 estos, será castigado con la pena de presidio menor en sus grados medio a máximo.

Este delito tiene como antecedente el artículo 3° del Convenio de Budapest, que señala: «Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático».

Los verbos denotativos de este tipo penal son «interceptar», «interrumpir» o «interferir», y, en el caso del inciso segundo, «captar». El objeto del delito es, en el inciso primero, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, y en el inciso segundo, los datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de estos.

Por otro lado, y al igual que en el caso de los delitos contemplados en el artículo 2° de la ley, se exige una actuación indebida, por lo que se concluye que podrían existir interceptaciones lícitas, llevadas a cabo por una persona facultada para ello.[58] Respecto a una posible comisión por omisión de este delito, nos remitimos a lo ya señalado en los acápites anteriores.

B. ITER CRIMINIS

En lo relativo a su estructura, el delito de interceptación ilícita es un delito de mera actividad, pues solo se exige la interceptación, interrup-

58 Mayer y Vera (2022b), p. 287.

ción o interferencia de una transmisión, sin que se demande un resultado material separado en el tiempo y en el espacio de tales conductas[59]. Al ser una conducta susceptible de fraccionamiento, cabe el castigo de la tentativa, mas no del delito frustrado.

C. SUJETO ACTIVO

La ley no realiza exigencias específicas respecto del sujeto activo, más allá de lo ya indicado con relación a que no debe encontrarse autorizado por el titular del sistema o los datos informáticos para interceptarlo o captarlos, respectivamente.

D. ASPECTO SUBJETIVO

Desde un punto de vista subjetivo, el tipo penal no contempla requisito subjetivo alguno que apunte, forzosamente, a demandar dolo directo (por ejemplo, una actuación realizada «maliciosamente»), de modo que basta con que el delito se cometa con dolo eventual. La modalidad culposa debe ser descartada, por las mismas razones indicadas respecto de otros delitos informáticos.[60]

2.3. Falsificación informática (artículo 5°, Ley 21.459)

Se revisará cada aspecto relevante por separado.

A) Conducta típica

El artículo 5° inciso primero de la Ley 21.459 consagra: «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». Esta conducta configura el delito de falsificación informática. Por su parte, el inciso segundo del mismo artículo dispone: «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 grado mínimo». Esta norma representa una figura agravada del mismo delito, en razón de la especial calidad del sujeto activo.

59 *Ídem.*
60 *Ídem.*

Al igual que los delitos de ataque a la integridad de los datos informáticos, acceso ilícito e interceptación ilícita, esta figura tiene su antecedente en el Convenio contra la Ciberdelincuencia, o Convenio de Budapest, que en su artículo 7° establece: «Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal».

El tipo penal regula un supuesto de «falsificación o, lo que es lo mismo, de falsedad», siendo posible definir la conducta delictiva como «una alteración de la verdad».[61] Ahora bien, no toda falsedad es penalmente relevante, sino que es necesario, además, que el objeto falseado, en este caso los datos informáticos, tenga vocación de entrada en el tráfico jurídico, trascendiendo la esfera íntima del individuo que realiza la falsedad.[62] Por ello, no constituye una falsedad, en el sentido señalado, el hecho de alterar un documento que el agente luego conserva en un armario al que ningún otro sujeto tiene acceso.[63]

Los verbos denotativos rectores de este tipo son «introducir», «alterar», «dañar» o «suprimir». Es interesante hacer dos comentarios aquí. Por un lado, la conjunción «o» permite señalar que el tipo está estructurado como uno de hipótesis alternativa, al igual que el resto de los delitos ya analizados *supra*. En segundo lugar, las cuatro conductas descritas se encuentran también contempladas en el artículo 1° de la ley, que prevé el delito de ataque a la integridad de un sistema informático, lo que trae como consecuencia que sea determinante la intención delictiva de que los datos introducidos, alterados, dañados o suprimidos por el autor del delito sean tomados como auténticos para efectos de determinar la aplicación de una u otra norma penal.

El tipo exige también que la conducta sea ejecutada «indebidamente», existiendo supuestos en los cuales una persona puede encontrarse facul-

61 Mayer y Vera (2022a), p. 264.
62 *Ídem.*
63 *Ídem.*

tada para dañar o suprimir datos, como por ejemplo en una hipótesis en la cual el titular de los datos solicita a un asistente que introduzca, en un documento electrónico en el que se contiene un contrato, una cláusula inicialmente no prevista en él.[64]

El objeto del delito son los datos informáticos y, con relación a hipótesis de castigo de posibles comisiones omisivas, estas deben ser descartadas por las mismas razones explicitadas respecto de los delitos ya estudiados.

B) Iter criminis

En cuanto a la estructura del tipo, puede afirmarse que la falsificación informática constituye un delito de mera actividad, toda vez que basta con que se lleve a cabo una introducción, una alteración, un daño o una supresión de datos para que se configure el tipo penal. Consiguientemente, ha de excluirse el castigo penal de la frustración; mientras que, como dichos comportamientos son fraccionables, cabe sostener que la tentativa sí es punible.[65]

C) Sujeto activo y pasivo

En el análisis de este punto es necesario distinguir entre la figura contemplada en el inciso primero del artículo 5° y aquella contemplada en el inciso segundo. Respecto de la primera, este sería un delito de sujeto indiferente, con la sola nota de que debe ser una persona que no cuente con la debida autorización para efectuar la conducta, como ya fue indicado *supra*. Por otra parte, el inciso segundo establece un delito especial, sancionando una figura calificada de este mismo delito, precisamente con relación a la calidad que debe investir el sujeto activo. Esta calidad es la de ser un empleado público, concepto que se encuentra definido de manera amplia en el artículo 260 del Código Penal: «todo el que desempeñe un cargo o función pública, sea en la Administración central o en instituciones o empresas semifiscales, municipales, autónomas u organismos creados por el Estado o dependientes de él, aunque no sean de nombramiento del Jefe de la República ni reciban sueldo del Estado».

64 Mayer y Vera (2022b), p. 291.
65 *Ídem.*

En lo relacionado con el sujeto pasivo, al ser este un tipo penal que regula una conducta de falsedad, el bien jurídico protegido sería, además de la información como objeto de protección jurídica, la funcionalidad documental y el normal funcionamiento del tráfico jurídico, siendo estos bienes jurídicos colectivos o supraindividuales respecto de los cuales no es posible identificar una víctima determinada.

D) Aspecto subjetivo

En el ámbito subjetivo, el inciso primero del tipo penal exige que se actúe con la *intención* de que los datos introducidos, alterados, dañados o suprimidos sean tomados como auténticos o utilizados para generar documentos auténticos. Esa forma de regular el dolo, en especial por la exigencia de que se actúe «para» generar documentos auténticos, puede entenderse como un reforzamiento del elemento subjetivo que equivale a una exigencia de dolo directo.[66]

Por otra parte, el inciso segundo exige que el empleado público que cometa el delito de falsificación actúe *abusando de su oficio*, lo que representa de igual forma una exigencia de dolo directo por parte del sujeto activo.

Debido a esto, y a los demás argumentos expuestos a propósito de los otros delitos informáticos, no es posible el castigo de comisiones culposas de esta figura delictiva.

2.4. Receptación de datos informáticos (artículo 6°, Ley 21.459)

Se revisará cada aspecto relevante por separado.

A) Conducta típica

Este delito está tipificado en el artículo 6° de la Ley 21.459, que dispone: «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».

66 Mayer y Vera (2022b), p. 292.

El delito de receptación informática es una figura delictiva que no tiene antecedentes directos en el Convenio de Budapest y que, en ese sentido, constituye un tipo penal original. No obstante tratarse de una figura inédita en el contexto de la criminalidad informática, la receptación como ilícito ya se encuentra regulada en la legislación penal chilena, en el ámbito de los delitos contra la propiedad (artículo 456 bis A del CP).[67] La razón que justificaría su inclusión en la Ley de Delitos Informáticos como un tipo penal autónomo es la inmaterialidad del objeto sobre el cual recae el delito, característica propia y distintiva de la criminalidad informática.[68] El contenido del delito se orienta, en primer lugar, a la evitación de la circulación indebida de información, intensificando así la afectación de la confidencialidad de los datos que fueron objeto de un delito informático antecedente, y, en segundo lugar, a impedir su empleo como instrumento para ulteriores comportamientos ilícitos.[69]

El tipo se estructura en torno a tres comportamientos alternativos, *comercialice, transfiera o almacene*, bastando la ejecución de cualquiera de las conductas para que se configure el delito. Todas ellos constituyen acciones, de modo que debe descartarse la receptación omisiva de datos informáticos,[70] tal como en el resto de los delitos informáticos.

B) Objeto material

El objeto sobre el cual recae la acción delictiva son los datos informáticos, con la particularidad de que estos deben provenir necesariamente de la realización de conductas susceptibles de ser calificadas como de acceso ilícito, espionaje informático, divulgación de datos obtenidos indebidamente, interceptación ilícita o falsificación informática, de una forma análoga a como lo exige el artículo 456 bis A del Código Penal respecto de la receptación común. Debido a esto, si los datos provienen de algún otro delito, informático o no, no será posible aplicar este tipo penal, por lo que el requisito asociado al origen de los datos configura un elemento objetivo del tipo.

Como una pequeña nota respecto a la penalidad asignada al delito de receptación informática, esta será determinada en atención al tipo penal

67 Mayer y Vera (2022b), p. 293.
68 Mayer y Vera (2022b), p. 294.
69 Bascur y Peña (2022), p. 4.
70 Mayer y Vera (2022b), p. 294.

base del cual provengan los datos informáticos, aplicándosele la pena que corresponda rebajada en un grado. Esto pone de manifiesto que para el legislador esta conducta constituiría un injusto menor respecto del de los tipos penales a los cuales este accede.

C) Iter criminis

En lo que respecta a la estructura del tipo, la receptación de datos informáticos corresponde a un delito de mera actividad, pues solo exige que se comercialicen, transfieran o almacenen datos, concurriendo ciertos requisitos, sin que se demande un resultado material. Teniendo en cuenta que ese comportamiento es fraccionable, es posible sostener que cabe el castigo de la tentativa.[71]

D) Sujeto activo y pasivo

Por razones sistemáticas, el autor del delito de receptación informática no puede ser el mismo sujeto que haya cometido los delitos contemplados en los artículos 2°, 3° y 5° de la Ley 21.459, existiendo un concurso aparente de leyes penales que se resuelve de acuerdo con el principio de subsidiaridad tácita. En resumen, si una persona intercepta o falsifica datos informáticos para luego almacenarlos, solo será castigado por la primera de estas conductas.

E) Aspecto subjetivo

Desde el punto de vista del dolo, el tipo exige que el sujeto activo actúe conociendo o no pudiendo menos que conocer el origen ilícito de los datos informáticos que comercialice, transfiera o almacene. En este sentido, el delito admite comisión tanto con dolo directo como con dolo eventual. De ello se sigue que se excluye el castigo de la receptación de datos informáticos si solo concurre culpa en el agente del comportamiento incriminado.[72]

Por otra parte, el tipo penal exige un elemento subjetivo propio, consistente en llevar a cabo las conductas consistentes en comercializar, transferir o almacenar los datos con una finalidad ilícita, o sea, antijurídica; ello se deriva de la expresión «con el mismo objeto u otro fin ilícito».

71 Mayer y Vera (2022b), p. 296.
72 *Ídem.*

2.5. Fraude informático (artículo 7°, Ley 21.459)

Cuando hablamos sobre el bien jurídico protegido en los delitos informáticos, mencionamos la clasificación que realiza la doctrina, y en cierta medida también la Ley 21.459, de las principales formas comisivas que adoptan esta clase de delitos, distinguiendo entre las conductas de sabotaje informático, espionaje informático y fraude informático. Respecto de esta última, dijimos que son aquellas conductas delictivas que implican alteración o manipulación de datos o programas de sistemas informáticos, afectando por tanto al bien jurídico propiamente informático, consistente en «la integridad, confidencialidad y disponibilidad de los sistemas informáticos, y de los datos contenidos en ellos». Sin embargo, también se señaló que la figura contemplada en el artículo 7° de la LDI es un delito cuya lesividad es difícil de determinar, ya que no solo afecta la información entendida como un valor merecedor de una especial protección por parte del ordenamiento jurídico, sino que principalmente atenta contra un bien jurídico individual, como lo es el patrimonio. En este sentido, el artículo 7° constituye la manifestación más reciente del esfuerzo legislativo por castigar los atentados patrimoniales ejecutados en el contexto de la expansión del comercio electrónico.[73]

A) Conducta típica

Este delito se encuentra regulado en el artículo 7° de la Ley 21.459, que establece:

> 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.

73 Bascur y Peña (2022), p. 4.

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.

Este delito tiene como antecedente el artículo 8° del Convenio de Budapest,[74] ya que no estaba contemplado expresamente en la derogada Ley 19.223. Esa ausencia resultaba especialmente problemática, puesto que, dentro de los delitos informáticos, este es el de mayor frecuencia práctica y el que más impacto genera en el sistema económico, llevando a algunos autores a considerarlo como un delito integrante de la criminalidad económica.[75]

De la lectura del artículo 7° de la Ley 21.459 fluye que el fraude informático se encuentra regulado sobre la base de dos tipos penales, consagrados en el inciso primero y en el inciso segundo de dicho artículo.

Respecto del delito contemplado en el inciso primero, cabe apuntar que el tipo penal referido representa una figura paralela a la estafa, en especial a la del delito de fraude del artículo 467 del Código Penal, ya que no obstante tener una naturaleza diversa en relación con la conducta delictiva,[76] constituyen ilícitos penales equivalentes desde el punto de vista de su gravedad y en ambos casos la pena aplicable se determina con relación al monto del perjuicio causado.

El verbo rector denotativo del delito de fraude informático propiamente tal es «El que *manipule*», lo que, de acuerdo con la RAE, puede entenderse como intervenir, en este caso, los datos informáticos, distor-

74 Artículo 8. Fraude informático: «Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona».

75 Mayer y Vera (2022b), p. 298.

76 *Ídem.*

sionando su configuración.[77] La misma norma establece las modalidades en que esta manipulación puede ser ejercida, ya sea mediante la «introducción», «alteración», «daño» o «supresión» de datos informáticos, o también a través de la acción genérica de interferir de cualquier forma sobre un sistema informático, que representaría el contenido fundamental de todos los actos de manipulación fraudulenta, esto es, la distorsión de la configuración del sistema informático objeto de incidencia.[78]

A partir de una lectura integral de la ley, resulta evidente que las conductas tipificadas como modalidades comisivas del delito de fraude informático ya están consideradas respecto de los delitos de sabotaje y espionaje informático, siendo decisivo para determinar la norma penal a aplicar la finalidad de obtener un beneficio económico para sí o para un tercero, elemento subjetivo propio que será analizado más adelante.

A nivel de derecho comparado, se han clasificado las modalidades de ejecución de fraude informático conforme al momento en que el autor incide sobre el proceso ejecutado por el respectivo sistema: durante el i) ingreso de los datos (*input*), mediante acciones tales como incorporar movimientos falsos, eliminar la entrada de operaciones reales o incorporar acreedores; actos perpetrados durante ii) el tratamiento o procesamiento de los datos ya ingresados, como la desfiguración (redondear sumas de dinero), efectuar asignaciones irregulares de dinero o eliminación de saldos negativos; y, finalmente, injerencias durante el iii) momento de emisión de los resultados exteriores del proceso (*output*).[79]

Un caso que ha generado discusión en la doctrina es aquel en que el autor utiliza datos reales para obtener una transferencia electrónica no consentida por el titular, como serían los casos de utilización abusiva o indebida de datos informáticos ajenos, generalmente ilícitamente obtenidos, pero sin ocasionar un funcionamiento incorrecto del sistema.[80] Se discute si la acción típica debe *interferir* en sentido estricto sobre el sistema, a través de actos de intrusismo y sabotaje, o bastaría el simple uso indebido de datos para cumplir con las exigencias del tipo penal, como sería el caso de quien obtiene ilegalmente claves personales de un tercero y las utiliza para acceder a su cuenta bancaria y ocasionarle

77 *Ídem.*
78 Bascur y Peña (2022), p. 19.
79 *Ídem.*
80 *Ídem.*

un perjuicio económico. Compartimos lo señalado por Bascur y Peña, en el sentido de que el verbo «introducir» permite incorporarla como conducta sancionable.[81]

Un elemento objetivo del tipo penal exigido por la ley para que se configure el fraude informático es el perjuicio económico de un tercero causado por la conducta delictiva. Dentro de la estructura del tipo, este perjuicio representa el resultado del delito, debiendo existir por tanto una relación de causalidad fáctica entre la conducta de manipulación de datos informáticos y el perjuicio. La ley solo señala «El que, causando un perjuicio a otro […]», sin especificar cuál debe ser la naturaleza de este perjuicio. Ahora bien, debido a que la pena del delito se determinará de acuerdo con el monto del perjuicio sufrido, parece obvio que este perjuicio debe tener un carácter económico.

Como delito de resultado, se exige que el perjuicio patrimonial sea producido mediante la acción de manipulación informática. La exigencia de esta relación de causalidad, nos parece, impide subsumir directamente bajo esta figura a todo el conjunto de acciones ejecutadas previamente para la obtención no consentida de la información del titular y necesaria para ejecutar las operaciones electrónicas defraudatorias, vale decir, de aquellas conductas informáticas que constituyen mecanismos anteriores o preparatorios de la acción típica.[82]

En este sentido, tales actos han sido categorizados en dos grupos de casos: aquellas conductas denominadas i) *phishing* o «pesca de claves», consistentes en la obtención de la información del perjudicado mediante a) engaño, persuasión o amenaza sobre este (correos electrónicos, SMS, mensajes de aplicaciones, etcétera) como también por b) la instalación subrepticia de un *software* malicioso en el sistema que la almacena; y los denominados actos de ii) *pharming*, esto es, la implantación de accesos y sitios web falsificados que permiten engañar al usuario para que ingrese por error sus datos reales y así estos puedan ser conocidos y registrados indebidamente por el autor.[83] Ahora bien, aunque estas conductas no podrían ser sancionadas a título de fraude informático por faltar la relación de causalidad entre la manipulación y el perjuicio, sí podrían ser sancionadas por algunos de los delitos contemplados en el artículo 7° de

81 *Ídem.*
82 *Ídem.*
83 *Ídem.*

la Ley 20.009, los cuales serán analizados más adelante. Todo esto sin perjuicio de que sea posible castigarlas a título de acceso ilícito, espionaje o falsificación informática si se cumple con las exigencias típicas de estos delitos.

Por último, la hipótesis prevista en el artículo 7° inciso segundo de la ley castiga a quien «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». Como señalan Mayer y Vera, esta figura regula, como tipo penal autónomo, un supuesto de participación en un fraude informático que ha sido elevado a la categoría de autoría. Ello se ve confirmado porque a él resulta aplicable la misma pena que prevé la figura del inciso primero, así como porque también se *considera* autor (de un fraude informático) a quien realiza la conducta en él descrita.[84]

La disposición tipifica actos de colaboración con la manipulación informática del inciso primero y fue incorporada a instancias del Ministerio Público, para zanjar la dificultad procesal de acreditar supuestos de coautoría concertada (artículo 15 números 1 o 3 del Código Penal) entre el colaborador y el autor del fraude. Específicamente, se buscó castigar a los denominados «muleros» o intermediarios electrónicos,[85] quienes intervienen aportando una cuenta bancaria propia para transferir el dinero obtenido por el fraude, permitiendo la desviación de los fondos electrónicos, generalmente sin conocer al autor originario y con ánimo de lucro.[86] El verbo rector denotativo de esta segunda figura delictiva del artículo 7° es «facilitar», lo cual implica una colaboración y aporte sustantivo a la comisión del delito realizado con anterioridad o de forma simultánea a la ejecución del fraude informático al cual esta conducta accede.

B) Iter criminis

De la exigencia de que se cause un perjuicio económico a la víctima del delito se extrae como consecuencia que estamos en presencia de un delito de resultado, cuyo objeto material son los datos informáticos y que, por tanto, admite el castigo de la tentativa y del delito frustrado.

84 Mayer y Vera (2022b), p. 298.
85 Bascur y Peña (2022), p. 19.
86 *Ídem.*

C) Sujeto activo y pasivo

El tipo penal utiliza la expresión «El que […]», por lo que es un delito de sujeto indiferente que en principio podría ser cometido por cualquier persona. Como ya se señaló, el fraude informático es un delito pluriofensivo que no solo afecta la disponibilidad de los datos informáticos o de un sistema informático, sino que fundamentalmente es un atentado contra el patrimonio de una o más personas determinadas, las cuales serán las víctimas del delito.

D) Aspecto subjetivo

En el plano subjetivo, a pesar de que la descripción del fraude informático requiere que se actúe con una determinada finalidad, exigencia que podría entenderse como una demanda de dolo, ella en realidad corresponde a un elemento del tipo o del injusto (elemento subjetivo propio), concretamente, al ánimo de lucro. En efecto, en el ámbito de los delitos contra intereses patrimoniales, actúa con ánimo de lucro el sujeto que busca obtener una utilidad o ventaja económica a través del comportamiento incriminado, idea que en nada difiere de la exigencia establecida en el artículo 7° inciso primero de la nueva Ley de Delitos Informáticos.[87]

Respecto del delito del inciso segundo del artículo 7°, el tipo regula una exigencia análoga a la contenida en la receptación informática, toda vez que demanda que el agente conozca o no pueda menos que conocer la ilicitud de la conducta constitutiva de fraude informático, que se regula en el inciso primero del artículo 7° de la nueva Ley de Delitos Informáticos. En ese sentido, es posible que el agente conozca esa ilicitud, en cuyo caso actuará con dolo directo, o bien no pueda menos que conocerla, en cuyo caso actuará con dolo eventual.[88]

E) Relaciones concursales

Desde la perspectiva concursal, es necesario distinguir la clase de delitos conjuntamente realizados. En primer lugar, con relación a los delitos establecidos en la Ley de Delitos Informáticos, los actos de acceso

87 Mayer y Vera (2022b), p. 300.
88 *Ídem.*

ilícito (artículo 2° inciso primero, primera oración) o espionaje (artículo 2° inciso primero, segunda oración) pueden verificarse como actos previos al fraude informático, mientras que los de sabotaje (artículos 2° y 4°) que coincidan con la descripción, como actos coetáneos a su ejecución. En ambos casos, atendido el contenido de injusto de las realizaciones involucradas, se debe considerar un concurso aparente de delitos.[89]

Por último, es importante destacar que el artículo 9° de la Ley 20.009 estableció de manera explícita que «Las penas establecidas en el artículo 7° de la ley se aplicarán sin perjuicio de las eventuales sanciones que también corresponda aplicar por los delitos contemplados en la Ley N° 19.223 [actual Ley 21.459], o aquella que la modifique, reemplace o sustituya en materia de delitos informáticos o ciberdelincuencia». En este sentido, el legislador quiso indicar a la persona encargada de juzgar estos delitos que estos representan contenidos de injusto diversos y, por ello, en caso de concurrencia de dos o más delitos, deberá estarse a las reglas del concurso ideal o real, según sea el caso.[90]

2.6. Abuso de los dispositivos (artículo 8°, Ley 21.459)

Se revisará cada elemento relevante de esta figura por separado.

A) Conducta típica

Este delito, que tiene como antecedente el tipo de abuso de los dispositivos del artículo 6° del Convenio de Budapest, se regula en el artículo 8° de la Ley 21.459, disposición que establece lo siguiente:

> El que para la perpetración de los delitos previstos en los artículos 1º a 4º de esta ley o de las conductas señaladas en el artículo 7º 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.

89 Bascur y Peña (2022), p. 22.
90 *Ídem.*

Lo que ha hecho el legislador con la tipificación de esta figura delictiva es elevar a la categoría de delito autónomo lo que en realidad constituye actos preparatorios de otros delitos informáticos,[91] en específico, los delitos de ataque a la integridad de un sistema informático (artículo 1° de la Ley 21.459), acceso ilícito (artículo 2° de la Ley 21.459), interceptación ilícita (artículo 3° de la Ley 21.459), ataque a la integridad de los datos (artículo 4° de la Ley 21.459) y los delitos contemplados en el artículo 7° de la Ley 20.009.

Su inclusión en el catálogo de delitos informáticos implica un adelantamiento de las barreras de protección de los intereses subyacentes a la criminalidad informática que, de no haberse establecido, habría determinado la impunidad de las conductas que en él se describen,[92] de manera similar a lo que hace el artículo 445 del Código Penal respecto del delito de robo.[93] Llama la atención la no inclusión del fraude informático (artículo 7° de la Ley 21.459) dentro del mencionado catálogo de delitos, no obstante lo cual se han planteado fórmulas para evitar este posible vacío de punición señalándose, por un lado, que los actos que constituyen una operación de manipulación informática defraudatoria igualmente resulten objeto de esta remisión como actos ejecutivos de los tipos de atentado contra la integridad de sistemas o datos informáticos (artículos 1° y 4°) y acceso ilícito (artículo 2°),[94] aprovechando que comparten las mismas conductas típicas, o, por otro lado, siendo previstas por el inciso segundo del artículo 7°, que sanciona la conducta consistente en facilitar los medios para la ejecución de dicho ilícito.[95]

Los verbos denotativos rectores de esta figura delictiva son «entregar», que de acuerdo con la RAE es dar una cosa a alguien o hacer que pase a tenerla; «obtener» (para su utilización), que puede entenderse como conseguir algunos de dichos objetos; «importar», que implica introducirlo al país desde el exterior; «difundir», entendido como sinónimo de divulgar, y «poner a disposición», que supone colocar alguno de los posibles objetos materiales del delito de forma tal que se encuentre apto y listo para un determinado fin, concretamente, como medio para la ejecución de alguno de los ilícitos penales indicados *supra*.[96]

91 Mayer y Vera (2022b), p. 300.
92 Mayer y Vera (2022b), p. 303.
93 Bascur y Peña (2022), p. 30.
94 Bascur y Peña (2022), p. 31.
95 Mayer y Vera (2022b), p. 304.
96 *Ídem.*

Las conductas de este tipo penal son de hipótesis alternativas, es decir, basta la verificación de cualquiera de ellas para que el delito se configure. Por otra parte, todas ellas implican la realización de movimientos corporales, siendo incompatibles con comisiones omisivas y descartando el castigo de la comisión por omisión de igual forma que en el resto de los delitos contemplados en la Ley 21.459.

B) Objeto material

El objeto material del delito pueden ser 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 alguno de los delitos que indica el legislador. En ese sentido, a pesar de que se trata de un listado que, al menos formalmente, está redactado en términos taxativos, se trata de objetos de tal amplitud (por ejemplo, por la referencia a «dispositivos» o a «datos») que prácticamente permiten incluir cualquier cosa que sea idónea para la comisión de aquellos ilícitos.[97] Es importante señalar que el tipo exige que dichos objetos deben haber sido creados o adaptados *principalmente* para la perpetración de algunos de los delitos indicados, lo que permite el castigo de aquellas conductas que recaigan sobre objetos que solo parcialmente se orientan a la comisión de los ilícitos mencionados.

C) Iter criminis

En cuanto a la estructura del tipo, puede afirmarse que el delito de abuso de los dispositivos constituye un tipo de mera actividad, pues solo exige que se lleve a cabo una entrega, una obtención (para su utilización), una importación, una difusión o una puesta a disposición para que se configure el tipo penal. Consiguientemente, ha de excluirse el castigo penal de la frustración, mientras que, como dichos comportamientos son fraccionables, cabe sostener que la tentativa sí es punible.[98]

D) Sujeto activo y pasivo

El artículo 8° de la Ley 21.459 no realiza ninguna exigencia respecto de la persona que comete el delito (sujeto activo) como tampoco respec-

97 *Ídem.*
98 *Ídem.*

to de la persona afectada por este (sujeto pasivo). Sí podemos señalar que, al constituir el abuso de los dispositivos un acto preparatorio para la comisión de otros delitos, la persona que comete el delito de abuso de los dispositivos no debe después cometer alguno de los delitos contemplados en este artículo y que estén tipificados en la Ley 21.459 (artículos 1° a 4°), porque en ese caso el injusto penal quedaría absorbido por este otro delito.

Si se comete el delito de abuso de dispositivos y luego el mismo sujeto ejecuta una conducta tipificada en el artículo 7° de la Ley 20.009, se aplicará la regla del artículo 9° de dicha ley, como se indicará a propósito de las relaciones concursales.

E) Relaciones concursales

Como ya fue señalado en el acápite anterior, si quien detenta el objeto lesivo también ejecuta alguno de los delitos informáticos previstos en la Ley 21.459, debe apreciarse un concurso aparente de leyes penales.[99] Ahora bien, debido al contenido del ya citado artículo 9° de la Ley 20.009, si el delito de abuso de los dispositivos, o cualquier otro delito informático de la Ley 21.459, es cometido por la misma persona que después comete alguno de los delitos contemplados en el artículo 7° de la Ley 20.009, estaremos en presencia de un concurso ideal, o bien de un concurso real o material de delitos, según las circunstancias del caso.

F) Aspecto subjetivo

En el plano subjetivo, el tipo penal exige que los comportamientos delictivos se lleven a cabo para la perpetración de los delitos que establece el legislador, exigencia que implica demandar dolo directo en el agente de la conducta típica. En ese sentido, el comportamiento que se lleva a cabo, y que opera como medio, debe tener como finalidad la perpetración de alguno de los delitos que especifica la ley, exigencia que no se satisface si solo concurre dolo eventual.[100]

Este elemento subjetivo desempeña la función de excluir de la tipicidad determinadas acciones habituales que son ejecutadas con *hardware* o *software* en el contexto empresarial y comercial, por ejemplo, con fines

99 Bascur y Peña (2022), p. 33.
100 Mayer y Vera (2022b), p. 305.

de investigación, ciberseguridad y entrenamiento, académico e inclusive policial,[101] como sería el caso de una empresa de ciberseguridad que obtuviere para su utilización códigos de seguridad para efectos de mejorar el servicio que entrega.

3. Tipos penales asociados a cibercriminalidad en otros cuerpos legales

Fuera de la LDI, existen tipos penales asociados a la cibercriminalidad, ya sea porque se cometen respecto de sistemas o datos informáticos, o se cometen por medio de ellos, que pertenecen a la categoría de delitos informáticos en sentido amplio. En los siguientes acápites nos referiremos en particular a los delitos contemplados en la Ley 20.009, haciendo especial referencia a las figuras de *phishing* y *pharming,* y al delito de violación de secreto previsto en el artículo 36 B letra f) de la ley general de telecomunicaciones.

3.1. Fraudes a través de tarjetas de pago y transacciones electrónicas

La Ley 20.009, que establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, robo, hurto o fraude, es otro cuerpo normativo de nuestro ordenamiento jurídico que contempla delitos relacionados con la criminalidad informática. Esta ley sufrió una importante modificación con la Ley 21.234, del año 2020, que introdujo variaciones con relación al ámbito de aplicación de la ley, ampliándolo a los fraudes en transacciones electrónicas y permitiendo a los usuarios de las tarjetas de pago limitar su responsabilidad en caso de hurto, robo, extravío o fraude siempre que den aviso oportuno al emisor. Además, alteró la carga de la prueba en los casos previstos por esta ley, debiendo ser el banco o la institución financiera que emitió la tarjeta de pago el que deba recopilar los antecedentes que den cuenta de dolo o culpa grave en la conducta del usuario; en caso contrario, la entidad tendrá la obligación de restituir el monto total defraudado.

Para efectos de esta ley, se entenderá como transacciones electrónicas «aquellas operaciones realizadas por medios electrónicos que origi-

101 Bascur y Peña (2022), p. 31.

nen cargos y abonos o giros de dinero en cuentas corrientes bancarias, cuentas de depósitos a la vista, cuentas de provisión de fondos, tarjetas de pago u otros sistemas similares, tales como instrucciones de cargo en cuentas propias para abonar cuentas de terceros, incluyendo pagos y cargos automáticos, transferencias electrónicas de fondos, avances en efectivo, giros de dinero en cajeros automáticos y demás operaciones electrónicas contempladas en el contrato de prestación de servicios financieros respectivo. Se comprenden dentro de este concepto las transacciones efectuadas mediante portales web u otras plataformas electrónicas, informáticas, telefónicas o cualquier otro sistema similar dispuesto por la empresa bancaria o el proveedor del servicio financiero correspondiente».

Además de estas modificaciones, la Ley 21.234 reformó las figuras penales de la Ley 20.009, modificando el artículo 7°, el cual quedó redactado, en ese momento, de la siguiente manera:

> Las conductas que a continuación se señalan constituyen delito de uso fraudulento de tarjetas de pago y transacciones electrónicas y se sancionarán con la pena de presidio menor en su grado medio a máximo y multa correspondiente al triple del monto defraudado:
>
> a) Falsificar tarjetas de pago.
> b) Usar, vender, exportar, importar o distribuir tarjetas de pago falsificadas o sustraídas.
> c) Negociar, en cualquier forma, tarjetas de pago falsificadas o sustraídas.
> d) Usar, vender, exportar, importar o distribuir los datos o el número de tarjetas de pago, haciendo posible que terceros realicen pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de las mismas.
> e) Negociar, en cualquier forma, con los datos, el número de tarjetas de pago y claves o demás credenciales de seguridad o autenticación para efectuar pagos o transacciones electrónicas, con el fin de realizar las operaciones señaladas en el literal anterior.
> f) Usar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, bloqueadas, en cualquiera de las formas señaladas en las letras precedentes.
> g) Suplantar la identidad del titular o usuario frente al emisor, operador o comercio afiliado, según corresponda, para obtener la autorización que sea requerida para realizar transacciones.

h) Obtener maliciosamente, para sí o para un tercero, el pago total o parcial indebido, sea simulando la existencia de operaciones no autorizadas, provocándolo intencionalmente, o presentándolo ante el emisor como ocurrido por causas o en circunstancias distintas a las verdaderas.

Asimismo, incurrirá en el delito y sanciones que establece este artículo el que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.

Este inciso final era particularmente relevante, ya que abarcaba la gran mayoría de los hechos constitutivos de *phishing* y de *pharming*, los cuales tienen gran presencia en la práctica delictiva de los criminales informáticos y no pueden ser sancionados de acuerdo con el tipo penal de fraude informático del artículo 7° de la Ley 21.459, debido a la exigencia de que exista una relación de causalidad entre la manipulación informática y el perjuicio patrimonial, causalidad que, como se verá, no se da a propósito de estas prácticas delictivas.

Posteriormente, la Ley 21.595, publicada el 17 de agosto del 2023, conocida como Ley de Delitos Económicos, dentro de la gran variedad de modificaciones que implementó, derogó, por medio del artículo 58, las letras a), b), c), d), e), y g) del inciso primero y derogó por completo el recién mencionado inciso segundo, además de modificar la letra f) del inciso primero, quedando solo la letra h) completamente inalterada. El texto resultante de esta modificación fue el siguiente:

a) Artículo 7°. Las conductas que a continuación se señalan constituyen delito de uso fraudulento de tarjetas de pago y transacciones electrónicas y se sancionarán con la pena de presidio menor en su grado medio a máximo y multa correspondiente al triple del monto defraudado: Derogado.
b) Derogado.
c) Derogado.
d) Derogado.
e) Derogado.
f) Usar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, bloqueadas, para realizar pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de ellas.

g) Derogado.
h) Obtener maliciosamente, para sí o para un tercero, el pago total o parcial indebido, sea simulando la existencia de operaciones no autorizadas, provocándolo intencionalmente, o presentándolo ante el emisor como ocurrido por causas o en circunstancias distintas a las verdaderas.

Esta modificación legal fue propuesta por parte de los académicos que intervinieron en la Comisión de Constitución de la Cámara de Diputadas y Diputados en el primer trámite constitucional de tramitación de la Ley 21.595, para evitar una duplicidad normativa con el nuevo artículo 468 del Código Penal, el cual forma parte de las modificaciones incorporadas por la nueva LDE y se enmarca en una reestructuración del tipo penal de estafa, recogiendo el profundo consenso doctrinario en torno a que la estafa es un engaño que produce en otro un error y que lo induce a ejecutar, omitir o tolerar una acción que importa una disposición patrimonial en perjuicio suyo o de un tercero, con el objetivo de obtener una ventaja o beneficio.[102] Lo anterior representa una genuina tipificación del delito de estafa, en contraposición a la forma en que tradicionalmente el Código Penal chileno había regulado este delito, esto es, como una colección de supuestos de engaño o de contextos donde se producen engaños, más que una efectiva tipificación del delito de estafa.[103]

En este contexto, el nuevo artículo 468 del Código Penal[104] viene a operar como complemento de la figura principal de estafa contemplada

102 BCN (2023), p. 155.
103 *Ídem.*
104 «Las penas del artículo anterior serán aplicadas también al que para obtener un provecho para sí o para un tercero irrogue perjuicio patrimonial a otra persona:

1. Manipulando los datos contenidos en un sistema informático o el resultado del procesamiento informático de datos a través de una intromisión indebida en la operación de este.

2. Utilizando sin la autorización del titular una o más claves confidenciales que habiliten el acceso u operación de un sistema informático, o

3. Haciendo uso no autorizado de una tarjeta de pago ajena o de los datos codificados en una tarjeta de pago que la identifiquen y habiliten como medio de pago.

Sin perjuicio de las penas que correspondan conforme al inciso anterior, sufrirá la pena de presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales el que obtenga indebidamente los datos codificados en una tarjeta de pago que la identifiquen y habiliten como medio de pago. La misma pena sufrirá el que los adquiera o ponga a disposición de otro a cualquier título.

En la investigación de los delitos previstos en este artículo será aplicable lo dispuesto en el artículo 8 de la ley N° 20.009.

Lo dispuesto en los incisos segundo y tercero de este artículo será aplicable si el hecho no tuviere mayor pena conforme a otra ley».

en el artículo 467 del mismo cuerpo normativo, con la misma estructura del delito de estafa (ánimo de lucro e irrogación de un perjuicio patrimonial) y se incorporan los elementos típicos de alteración de funcionamiento de sistemas informáticos que tiene como resultado la irrogación de un perjuicio patrimonial para otra persona. Esto se encuentra en los tres primeros números del inciso segundo que se proponen, tal como están previstas en el derecho comparado y en la práctica chilena: manipulación de datos a través de intromisión indebida a los sistemas informáticos, utilización de claves sin autorización, uso de datos de tarjetas de pago y casos de clonación de tarjetas, por ejemplo.[105]

En resumen, lo que hizo la LDE fue trasladar las hipótesis delictivas antes previstas en el artículo 7° de la Ley 20.009 al Código Penal, al considerarse aquellas meras modalidades comisivas del delito de estafa. Es importante también destacar que de acuerdo con el artículo 2° numeral 7 de la LDE, los delitos que quedaron en las letras f) y h) de la Ley 20.009 constituyen delitos económicos de segunda categoría y les son aplicables las normas dispuestas para esta categoría de delitos.

Finalmente, el 30 de mayo de 2024, se publicó la Ley 21.673, la cual alteró nuevamente la estructura del art. 7° de la Ley N° 20.009, quedando la norma vigente de la siguiente manera:

Artículo 7.- Las conductas que a continuación se señalan constituyen delito de uso fraudulento de tarjetas de pago y transacciones electrónicas, y se sancionarán con la pena de presidio menor en su grado medio a máximo y multa correspondiente al triple del monto defraudado:

a) Usar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, bloqueadas para realizar pagos, transacciones electrónicas, giros en cajeros automáticos, o cualquier otra operación que corresponda exclusivamente al titular o usuario de ellas.
b) Obtener maliciosamente, para sí o para un tercero, la cancelación indebida de los cargos o la restitución indebida de fondos a que se refiere el artículo 5° de esta ley, sea proporcionando datos o antecedentes falsos en la declaración jurada a que se refiere el artículo 4° de esta ley, desconociendo falsamente una o más operaciones con medios de pago de su titularidad, simulando la existencia de operaciones no autorizadas, provocándolas intencionalmente, o

105 BCN (2023), p. 156.

presentándolas ante el emisor como ocurridas por causas o en circunstancias distintas a las verdaderas.

Como se puede apreciar, los tipos penales de la Ley 20.009 han experimentado una gran cantidad de modificaciones legales en el último tiempo, y consideramos importante hacer una nota sobre la evolución de estas figuras penales para efectos de obtener una acertada comprensión de los mismos.

A) Conducta típica

Antes de entrar a analizar en detalle las conductas punibles previstas en la Ley 20.009, se analizarán brevemente dos de las conductas de cibercrimen más comunes utilizadas por los delincuentes informáticos, el *phishing y el pharming,* para posteriormente identificar si estas conductas están cubiertas por los delitos tipificados en esta ley o por algún otro contemplado por nuestro ordenamiento jurídico.

El *phishing* es una técnica común de ciberdelincuencia que suele consistir en el envío de un correo electrónico a los objetivos con un enlace a un sitio web para que los usuarios hagan clic, lo que ocasiona la descarga de un *malware* en los dispositivos digitales de los usuarios o envía a los usuarios a un sitio web malicioso diseñado para robar sus credenciales. El sitio web «falsificado» (o sitio web *pharmed*) se parece al sitio web de la organización y/o agencia y solicita al usuario que ingrese las credenciales de inicio de sesión. El correo electrónico proporciona diferentes indicaciones para provocar miedo, pánico y/o una sensación de urgencia para que el usuario responda al correo electrónico (y complete las tareas solicitadas en el correo electrónico) lo antes posible, tales como la necesidad de actualizar la información personal para recibir fondos u otros beneficios, advertencias de actividad fraudulenta en la cuenta del usuario y otros eventos que requieran la atención inmediata del objetivo.[106]

En el *phishing* es habitual que el delincuente informático finja ser una institución bancaria y, en el momento en el que el usuario intente saber si se trata de un error o confusión y dé clic en algún enlace incluido en el correo recibido, será dirigido a otro sitio web que simula ser oficial, momento en el cual se le solicita completar formularios, además de ingresar a su cuenta, entregándole así sus datos bancarios al ciberdelincuente.[107]

106 Oficina de las Naciones Unidas contra la Droga y el Delito (2022), p.46.
107 Espacios de México (s.f.), s.p.

Por otra parte, el *pharming* consiste en la implantación de accesos y sitios web falsificados que permiten engañar al usuario para que ingrese por error sus datos reales y estos puedan ser conocidos y registrados indebidamente por el autor[108]. En esta técnica delictual, los *hackers*, a través de un *software* malicioso, intervienen directamente el servidor Domain Name System (DNS), el cual se encarga de direccionar al usuario al sitio que busca por medio de su navegador web. Por esta razón, esta técnica resulta ser más peligrosa, pues es más difícil de identificar.[109] Al igual que en el *phishing*, el objetivo del *pharming* consiste en apropiarse de información personal del usuario, por lo general, de datos bancarios.

Aunado a lo anterior, en algunas ocasiones el *pharming* es reforzado con técnicas de *phishing* como los ya mencionados correos electrónicos de instituciones bancarias con calidad de urgencia donde se dirige al usuario a un sitio no oficial. Normalmente, el *pharming* concluye cuando el delincuente utiliza la información bancaria del usuario para realizar una transferencia de fondos de alguna de sus cuentas, hacer alguna compra o alguna otra actividad que será cubierta con el dinero de la cuenta.[110]

Antes de la entrada en vigencia de la Ley 21.595, la doctrina y la jurisprudencia estimaban que estas conductas delictivas debían ser sancionadas de acuerdo con el inciso segundo del artículo 7° de la Ley 20.009, que rezaba: «Asimismo, incurrirá en el delito y sanciones que establece este artículo el que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas».

Debido a la derogación que hizo el artículo 58 de la nueva Ley de Delitos Económicos de esta norma, y también de parte importante del artículo 7° de la Ley 20.009, es necesario preguntarse cuál es la hipótesis normativa vigente que permite captar estas prácticas delictivas.

Antes de la entrada en vigencia de la Ley 21.234, en el año 2020, la doctrina había realizado diversos intentos por tratar de encapsular las

108 Bascur y Peña (2022), p. 21.
109 Espacios de México (s.f.), s.p.
110 *Ídem.*

conductas de *phishing* y *pharming* en alguno de los delitos contra la propiedad regulados en el Código Penal, debido a que los tipos penales contemplados por la Ley 20.009, en ese entonces, no preveían la sanción de penal de la obtención y uso de claves sustraídas.

Una de las opciones planteadas fue la de considerar que el uso de la clave de entrada al sistema bancario, facilitada con el consentimiento inválido del titular de la cuenta *(«pinpass»)*, podía constituir «uso de llaves falsas» en el sentido del delito de robo con fuerza en las cosas.[111] Esta alternativa debe ser rápidamente descartada, ya que, para que esto sea posible, se necesitaría un concepto extensivo de la llave falsa como el que contempla el artículo 239 del CP español[112] y resulta un forzamiento incompatible con el principio de legalidad aplicar esta solución en el sistema chileno. Por otra parte, la imposibilidad de entender esto último como un lugar «físico», porque es obvio que es «virtual», unido al hecho de que la clave se entrega con consentimiento del titular (viciado o en situación de error), excluye toda posibilidad de imputación por este título.[113]

También se planteó como posibilidad de imputación la relativa a los delitos de hurto y administración desleal, entre otros, pero sin duda el esfuerzo más relevante fue aquel relacionado con la antigua figura del delito de estafa. Como ya fue introducido en las páginas anteriores, nuestro CP, antes de la modificación incorporada por la Ley 21.595, establecía un sistema casuístico para regular el delito de estafa, utilizando ejemplos de conductas defraudatorias. Evidentemente, dada la antigüedad del Código Penal, que data del año 1874, ninguno de estos ejemplos hacía referencia a la coloquialmente llamada «estafa informática». Por este motivo, un sector de la doctrina recurría al entonces artículo 473 del CP,[114] que tradicionalmente fue considerado como una figura de estafa residual, en la cual tenían cabida todos los actos defraudatorios que no estuvieran contemplados expresamente en los ejemplos utilizados por la ley.

---

111 Oxman (2013), pp. 211-262.

112 Artículo 239.3 inciso 2°: «A los efectos de este artículo, se consideran llaves las tarjetas, magnéticas o perforadas, los mandos o instrumentos de apertura a distancia y cualquier otro instrumento tecnológico de eficacia similar».

113 *Ídem.*

114 «El que defraudare o perjudicare a otro usando de cualquier engaño que no se halle expresado en los artículos anteriores de este párrafo, será castigado con presidio o relegación menores en sus grados mínimos y multas de once a veinte unidades tributarias mensuales».

Doctrinalmente, se considera que el delito de estafa consta de cuatro elementos constitutivos: 1) el engaño, 2) el error, 3) la disposición patrimonial y 4) el perjuicio, elementos que a su vez deben estar vinculados por una relación de causalidad compleja, en la que el engaño sea la causa directa del error, así como el error de la disposición patrimonial y esta última del perjuicio.

Para que exista un engaño, debe existir una interlocución entre sujetos, debiendo aparecer un grado mínimo de interacción y comunicación entre personas.[115] Esta exigencia nos permite excluir de plano aquellas conductas donde se ataca directamente al sistema informático para generar el perjuicio, como es el caso del fraude informático (artículo 7°, Ley 21.459), o los supuestos de *pharming*. En el caso del *phishing*, esta interacción sí existe y produce un error en la víctima que consiste en entregar sus claves bancarias. Ahora, la dificultad se presenta respecto del tercer elemento, ya que la disposición patrimonial no es realizada por quien sufre el engaño, sino por quien lo ejecuta, ya que la mera entrega de las claves bancarias no constituye una disposición patrimonial, siendo a lo más el medio para que esta se lleve a cabo.

Por las razones recién expuestas, la conclusión que existía antes de la Ley 21.234 es que mientras no existiera una regulación expresa de la estafa informática, con la suficiente flexibilidad para hacerse cargo de otros problemas que puedan tener eventualmente lugar a través de la utilización indebida de las plataformas de banca *online*, las conductas de *phishing* y *pharming* eran atípicas en el modelo de estafa establecido en el CP.[116]

En este contexto, primero la Ley 21.234, al incluir el ya reiterado inciso final del artículo 7° de la Ley 20.009, y luego la Ley 21.595, con la modificación realizada a la estafa del CP, se hicieron cargo de este problema, quedando, a nuestro juicio, la conducta de *phishing* contemplada en el inciso tercero del artículo 468 CP, que castiga a quien «obtenga indebidamente los datos codificados en una tarjeta de pago que la identifiquen y habiliten como tarjeta de pago».

Por otra parte, el *pharming* estaría sancionado por el número 1 del inciso segundo del mismo artículo 468 CP, que castiga a quien «para obtener un provecho para sí o para un tercero irrogue perjuicio patri-

115 Oxman (2013), p. 252.
116 *Ídem.*

monial a otra persona: 1. Manipulando los datos contenidos en un sistema informático o el resultado del procesamiento informático de datos a través de una intromisión indebida en la operación de este».

Despejado el punto anterior, ahora es posible centrarse en los tipos penales que quedaron en la Ley 20.009 después de las modificaciones hechas por la Ley 21.595 y por la Ley 21.673. Estos son, por un lado, el artículo 7° letra a), que consagra: «Usar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, bloqueadas, para realizar pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de ellas». Aquí, el verbo denotativo rector del tipo es «usar», y el objeto material sobre el que recae la conducta son las tarjetas de pago o claves y demás credenciales de seguridad o autenticación, bloqueadas.

Por otra parte, el artículo 7° letra b) tipifica como delito «Obtener maliciosamente, para sí o para un tercero, la cancelación indebida de los cargos o la restitución indebida de fondos a que se refiere el artículo 5° de esta ley, sea proporcionando datos o antecedentes falsos en la declaración jurada a que se refiere el artículo 4° de esta ley, desconociendo falsamente una o más operaciones con medios de pago de su titularidad, simulando la existencia de operaciones no autorizadas, provocándolas intencionalmente, o presentándolas ante el emisor como ocurridas por causas o en circunstancias distintas a las verdaderas.».

En este caso, el verbo denotativo rector del tipo es «obtener», y el objeto material sobre el que recae es la cancelación indebida de los cargos o la restitución indebida de fondos. Cabe notar que aquí, a diferencia de la figura de la letra a), sí se modificó el tipo penal por parte de la Ley 21.673, lo cual responde a una demanda por parte de los bancos de castigar penalmente a aquellos usuarios que soliciten, con base en antecedentes falsos, la devolución de fondos en caso de fraude, aprovechándose de la presunción de responsabilidad de las instituciones financieras establecido en el artículo 5° de la Ley 20.009.

B) Iter criminis

Ambas figuras son delitos de resultado y, en consecuencia, compatibles con la sanción de la tentativa y del delito frustrado.

C) Sujeto activo y pasivo

El tipo penal no realiza exigencias relativas al sujeto activo y es, por tanto, un delito de sujeto indiferente. Con relación a la víctima, estos corresponden a delitos informáticos en sentido amplio y el bien jurídico protegido es el patrimonio; por lo tanto, el sujeto pasivo será quien sufra el perjuicio.

D) Aspecto subjetivo

En lo relativo al dolo, ambos tipos penales exigen dolo directo, al utilizar la expresión «maliciosamente». El artículo 7° letra a), además, exige una especial intención en el uso malicioso de las tarjetas de pago, ya que este uso debe ser realizado «para realizar pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de ellas». Cualquier uso malicioso de una tarjeta de pago que no sea realizado para realizar pagos o transacciones electrónicas no será punible, al faltar un elemento subjetivo propio del tipo.

3.2. Delito de violación de secreto en la Ley General de Telecomunicaciones

Otro delito incorporado por la Ley 21.459 es el delito de violación del deber de reserva previsto en los artículos 218 bis, 219 y 222 del Código Procesal Penal; no obstante, el legislador decidió colocar esta figura fuera de la Ley de Delitos Informáticos e introducirla en la Ley General de Telecomunicaciones (Ley 18.168).

A) Conducta típica

El artículo 36 B de la Ley 18.168 dispone: «Comete delito de acción pública: […] f) Los que vulneren el deber de reserva o secreto previsto en los artículos 218 bis, 219 y 222 del Código Procesal Penal, mediante el acceso, almacenamiento, o difusión de los antecedentes o la información señalados en dichas normas, serán sancionados con la pena de presidio menor en su grado máximo».

Para comprender cabalmente esta figura, es necesario identificar el contenido normativo de las normas referidas por el tipo penal, los artículos 218 bis, 219 y 222 del Código Procesal Penal. En primer lugar, el

artículo 218 bis es una de las modificaciones realizadas por la Ley 21.459 y entró en vigencia el 21 de junio del año 2024. Esta norma[117] prevé una nueva herramienta investigativa para el Ministerio Público, el que, con ocasión de una investigación penal, podrá requerir a cualquier proveedor de servicio[118] la conservación o protección de datos informáticos incluidos en un sistema informático que se encuentre a su disposición, durante el tiempo de espera necesario para obtener la debida autorización judicial. Se establece también un deber para la empresa requerida de colaborar y guardar secreto sobre el desarrollo de esta diligencia.

Por otra parte, el artículo 219 dispone que el juez de garantía, a petición del fiscal, podrá autorizar que cualquier empresa de telecomunicaciones facilite copias de las comunicaciones transmitidas o recibidas por ella y podrá ordenar la entrega de las versiones que existieren de las transmisiones de radio, televisión u otros medios.[119] Por último, el artículo 222 establece la diligencia de investigación conocida como interceptación de comunicaciones, que en su inciso sexto consagra una serie de deberes para las empresas concesionarias de servicios públicos de telecomunicaciones y prestadoras de servicios de Internet, entre los que se encuentran los siguientes:

A) Cumplir con esta medida, lo que incluye otorgar las facilidades necesarias al funcionario a cargo de la diligencia.
B) Mantener en carácter reservado y bajo las medidas de seguridad

117 Artículo 218 bis: «Preservación provisoria de datos informáticos. El Ministerio Público con ocasión de una investigación penal podrá requerir, a cualquier proveedor de servicio, la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega. Los datos se conservarán durante un período de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días. La empresa requerida estará obligada a prestar su colaboración y guardar secreto del desarrollo de esta diligencia».

118 Artículo 15 letra c), Ley 21.459: «Prestadores de servicios: Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo».

119 Artículo 219: «Copias de comunicaciones o transmisiones. El juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa de comunicaciones facilite copias de las comunicaciones transmitidas o recibidas por ellas. Del mismo modo, podrá ordenar la entrega de las versiones que existieren de las transmisiones de radio, televisión u otros medios».

correspondientes, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados.

C) Destruir dicha información una vez transcurrido el plazo máximo de mantención de estos datos.

D) El deber de los encargados de realizar la diligencia y de los empleados de las empresas mencionados de guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento.

Por lo tanto, estos constituyen los deberes de reserva, que, una vez infringidos, configuran el delito de violación de secreto contemplado en el artículo 36 B de la Ley 18.168.

El verbo denotativo rector del tipo penal es «vulnerar», que, de acuerdo con la RAE, significa transgredir, quebrantar o incumplir una ley o precepto. A su vez, esta transgresión puede ser ejecutada por medio del «acceso», «almacenamiento» o «difusión» de los antecedentes o la información señalados en los artículos ya mencionados del CPP. Como puede apreciarse, es un delito de hipótesis alternativa en el que la realización de cualquiera de las modalidades comisivas descritas permite entender por consumado el delito.

El objeto jurídico protegido es la confidencialidad de la información, y en este sentido pertenecería a la categoría del «espionaje informático», con la gran diferencia de que en este delito quien accede, almacena o difunde la información es alguien que carga con un deber de reserva respecto de esos datos y, por lo tanto, pertenece también a la categoría de los delitos de infracción de deber.

B) Iter criminis

El delito analizado corresponde a un delito de mera actividad, ya que el tipo no exige la causación de ninguna alteración en el mundo externo que sea distinguible de la ejecución misma de la conducta. Por su parte, el objeto material sobre el que recae la conducta serían los antecedentes e información requeridas por el Ministerio Público en el marco de una investigación penal.

C) Sujeto activo y pasivo

Como ya fue deslizado en los párrafos anteriores, este corresponde a un delito de infracción de deber, donde el factor de atribución determinante para que se configure este delito es el deber de reserva que el sujeto activo debe tener respecto de los antecedentes y de la información accedida, almacenada o difundida. Por lo tanto, es un delito especial, que no puede ser cometido sino por quien tenga este deber de reserva o secreto.

Una persona que no tenga este deber y acceda, almacene o difunda la información referida en los artículos 218 bis, 219 y 222 del CPP, podría, en el caso de que cumpla con el resto de los requisitos del tipo, ser sancionada a título de acceso ilícito, de espionaje informático o de divulgación de datos obtenidos ilegalmente, según las circunstancias del caso.

Con relación al sujeto pasivo, ya fue señalado que este delito puede ser ubicado dentro de la categoría de espionaje informático y, en consecuencia, el bien jurídico protegido sería la confidencialidad de los datos y el titular de estos la víctima del delito. Ahora bien, una correcta comprensión del delito en atención a su ubicación, a los deberes con los que se encuentra relacionado y a los objetivos político-criminales detrás de la ley, nos permite ver que el delito también protege un bien jurídico supraindividual y colectivo que, en nuestra opinión, sería la administración de justicia en su faz de protección a la correcta y eficiente investigación penal que permita, en definitiva, el esclarecimiento de los ilícitos.

Un argumento de texto para sostener esta postura se encuentra en la última frase del artículo 218 bis del Código Procesal Penal, que señala: «[…] La empresa requerida estará obligada a prestar su colaboración y guardar secreto del desarrollo de esta diligencia». Esta regla les impone a los prestadores de servicios un deber de secreto no solo respecto de los datos requeridos, sino también con relación a la diligencia de investigación, procurando la mayor eficacia posible de la misma.

D) Aspecto subjetivo

Respecto de la culpabilidad, el tipo penal no describe ningún tipo de exigencia de carácter subjetivo, por lo que habilita el castigo de conductas ejecutadas con dolo eventual. Sobre la posible comisión culposa de este delito, no existe ninguna norma que establezca de forma expresa su

castigo, lo cual nos permite descartar la sanción de conductas no dolosas de este delito.

3.3. Delitos cometidos a través de medios tecnológicos asociados a la explotación sexual comercial y la pornografía de niños, niñas y adolescentes y otros que afectan la privacidad e intimidad de las personas.

Como ya ha sido señalado en más de una ocasión a lo largo de este trabajo, los delitos informáticos pueden clasificarse *grosso modo* en dos categorías: delitos informáticos en sentido amplio y delitos informáticos en sentido estricto.[120] Dentro de la primera categoría, encontramos aquellos delitos que protegen bienes jurídicos individuales, que consisten en comisiones digitales de delitos ya existentes. El inexorable avance de la tecnología ha traído consigo cambios en las prácticas delictivas, y un área en la cual estos cambios traen riesgos particularmente agravados la encontramos en los delitos contra la integridad sexual.

Prácticas como el *grooming*, el acoso cibernético o la difusión de pornografía infantil a gran escala representan desafíos de primera importancia para los sistemas de persecución penal, en atención a los bienes jurídicos que estos delitos protegen. En las siguientes páginas se expondrán las principales modificaciones legales sustantivas introducidas por la Ley 21.522, que incorporó la tipificación del delito de transmisión de conductas sexuales a través de servicios de videoconferencia, telefonía o plataformas de *streaming* (artículo 367 septies) y la ampliación del delito de abuso sexual sin contacto (artículo 366 quáter).

La Ley 21.522, publicada el 30 de diciembre de 2022, introdujo cambios importantes en la regulación de los delitos relativos a la explotación comercial y material pornográfico de niñas, niños y adolescentes, incorporando un nuevo párrafo 6 bis, en el Título VII del Libro II del Código Penal.

Esta modificación legal, originada en un mensaje presidencial,[121] estuvo destinada, por una parte, a incorporar en la tipificación de los de-

120 En este sentido se dice que la tecnología puede ser la víctima del delito, el medio para cometerlo o una herramienta utilizada en su comisión.

121 Boletín 14.440-07, que introduce un nuevo Párrafo en el Título VII del Libro II del Código Penal, relativo a la explotación sexual comercial y material pornográfico de niños, niñas y adolescentes, iniciado por Mensaje Presidencial el 23 de junio de 2021, disponible en https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8098/

litos relativos a la explotación sexual comercial de niños, niñas y adolescentes (desde ahora, ESCNNA), una comprensión más desarrollada del fenómeno y, por otra, a actualizar las técnicas de investigación a una criminalidad en constante cambio, como todos los ciberdelitos.

La nueva normativa abandona definitivamente conceptos como *prostitución* (artículo 367 CP) y *servicios sexuales* (artículo 367 ter CP), que «favorecen la percepción y entendimiento –erróneo, por cierto– de que las niñas, niños o adolescentes presentan algún nivel de 'voluntariedad' para 'participar' en la comisión de estos delitos».[122] De la misma forma, entiende que la ESCNNA tiene características propias, que la diferencian de los otros delitos de violencia sexual. Por este motivo incorpora un nuevo párrafo 6 bis dentro del Título VII del Libro II del CP, que separa estos ilícitos del estupro y abusos sexuales y tipifica todas las figuras penales, en un mismo artículo, considerando que los delitos asociados al material pornográfico, es una modalidad de la ESCNNA.

Esta nueva configuración entrega argumentos de texto que permiten sostener que las conductas constitutivas de ESCNNA, además de afectar la libertad/indemnidad sexual, atentan contra la dignidad humana.[123] Refuerza lo anterior que la ESCNNA ha sido definida como una de las violaciones más severas a los derechos humanos de niñas, niños o adolescentes, siendo descrita por la ley chilena como «una forma de coacción y violencia contra los niños, niñas y adolescentes y una forma contemporánea de esclavitud».[124]

Desde el punto de vista sustantivo de la criminalidad informática, las modificaciones más importantes son la tipificación del delito de transmisión de conductas sexuales a través de servicios de videoconferencia, telefonía o plataformas de *streaming* (artículo 367 septies) y la ampliación del delito de abuso sexual sin contacto (artículo 366 quáter).

---

122 Mensaje Presidencial, pp. 5 y 6, disponible en https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8098/

123 Un mayor desarrollo en los documentos *Guía para el abordaje de los delitos de explotación sexual comercial de niñas, niños y adolescentes: aspectos fenomenológicos, victimológicos y marco normativo* (2021) y *Delitos relativos al material pornográfico en cuya elaboración hubieren sido utilizadas niñas, niños o adolescentes: Revisión normativa, de doctrina y de jurisprudencia* (2022). Disponibles en el Repositorio de Unidades de la Academia de la Fiscalía de Chile: https://agenda.minpublico.cl/academiafiscalia/repositorio-de-unidades/.

124 Ley 21.430, sobre garantías y protección integral de los derechos de la niñez y adolescencia. Artículo 37, inciso cuarto.

A. TRANSMISIÓN DE CONDUCTAS SEXUALES DE UNA PERSONA MENOR DE 18 AÑOS

EL ARTÍCULO 367 SEPTIES ESTABLECE:

> El que usando dispositivos técnicos transmitiere la imagen o sonido de una situación o interacción que permitiere presenciar, observar o escuchar la realización de una acción sexual o de una acción de significación sexual, por parte de una persona menor de dieciocho años, será sancionado con presidio menor en su grado máximo.

Este nuevo delito surgió durante la tramitación legislativa, en consideración a que el desarrollo tecnológico ha permitido nuevas formas de comisión de los delitos de violencia sexual, como la transmisión instantánea (en vivo) de contenidos sexuales a través de servicios de videoconferencia, telefonía o plataformas de *streaming*, en los que no quedan registros de imagen, audio o video que puedan ser considerados material pornográfico.[125]

A) Conducta típica

El verbo denotativo rector del tipo penal es «transmitir». Esta transmisión se debe efectuar a través de cualquier dispositivo técnico que permita presenciar, observar o escuchar en vivo o de forma instantánea las acciones.[126] En la tramitación legislativa se dieron como ejemplos el uso de *webcam*, la plataforma Zoom o servicios de *streaming*.[127] Por otra parte, el objeto material del delito son las imágenes o sonidos de acciones sexuales o de significación sexual en que participe una persona menor de dieciocho años.

La norma no exige que existan personas destinatarias de esta transmisión. Si bien fue discutido durante la tramitación legislativa, a petición del Ministerio Público se eliminaron las referencias contenidas en la propuesta inicial a «otra persona» y «número considerable o indeterminado de personas», dado que «lo que importa es simplemente el acto de trasmitir».[128]

---

125 Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento de la Cámara de Diputadas y Diputados. Primer Trámite Constitucional, p. 25. https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8098/

126 Informe de la Comisión de Constitución, p. 39 y ss.

127 Comisión de Constitución, p. 25 y 40.

128 Comisión de Constitución, p. 39.

B) Aspecto subjetivo

No se exige elemento subjetivo adicional alguno. Al igual que los delitos de participación en la producción y de comercialización, importación, exportación, distribución, difusión y exhibición de material pornográfico, es perfectamente imaginable la comisión del ilícito con dolo eventual respecto a la edad de las niñas, niños o adolescentes, o el hecho de estar efectivamente transmitiendo las conductas por alguna plataforma.

C) Penalidad

La pena asignada a este delito es la de presidio menor en su grado máximo, asimilando la pena a la de los delitos relativos al material pornográfico.

Cabe indicar que, a diferencia de lo que ocurre con la participación en la producción de material pornográfico, esta figura no queda cubierta en la excusa legal absolutoria establecida en el artículo 4° de la Ley 20.084.

B. DELITO DE ABUSO SEXUAL SIN CONTACTO

EL ARTÍCULO 366 QUÁTER ESTABLECE:

> El que, sin realizar una acción sexual en los términos anteriores, para procurar su excitación sexual o la excitación sexual de otro, realizare acciones de significación sexual ante una persona menor de catorce años, será castigado con presidio menor en su grado medio a máximo.
>
> Si se determinare a una persona menor de catorce años a realizar acciones de significación sexual delante suyo o de otro, o se la hiciere ver o escuchar material pornográfico o de explotación sexual o presenciar espectáculos del mismo carácter, la pena será presidio menor en su grado máximo.
>
> Será sancionado con la misma pena del inciso precedente al que determinare a una persona menor de catorce años a enviar, entregar o exhibir:
>
> a) Imágenes o grabaciones en que se representaren acciones de significación sexual de su persona o de otro menor de catorce años de edad.
> b) Imágenes o grabaciones de sus genitales o los de otra persona menor de catorce años.

A) Conducta típica

Se crean nuevas hipótesis de este delito consistentes en determinar a enviar, entregar o exhibir imágenes o grabaciones de los genitales de una niña o niño, o los de otra persona menor de catorce años.

El verbo denotativo rector de la conducta es «determinar», que se entiende como formar en el niño o niña la voluntad de enviar, entregar o exhibir imágenes o grabaciones de los genitales.

B) Aspecto subjetivo

Se mantiene la pena de presidio menor en su grado medio a máximo y la exigencia de ánimo especial (*para procurar su excitación sexual o la excitación sexual de otro*) en el caso de realizar acciones de significación sexual ante niñas o niños.

Se mantiene la pena de presidio menor en su grado máximo, pero se elimina la exigencia de ánimo especial (*para procurar su excitación sexual o la excitación sexual de otro*) en las hipótesis siguientes:

a) Determinar a niñas o niños a realizar acciones de significación sexual delante de sí o de otro.
b) Determinar a enviar, entregar o exhibir imágenes o grabaciones en que se representaren acciones de significación sexual de su persona o de otro menor de catorce años de edad.

Se aumenta la pena de presidio menor en su grado máximo y se elimina la exigencia de ánimo especial (*para procurar su excitación sexual o la excitación sexual de otro*) en el caso de hacer ver o escuchar material pornográfico o de explotación sexual o presenciar situaciones del mismo carácter.

Cabe indicar que se mantienen los antiguos incisos tercero (mismas penas en el caso de adolescentes, si concurren alguna de las circunstancias descritas en dicho inciso), cuarto (comisión de delitos a distancia por medio electrónico) y quinto (regla de determinación de pena especial, aumentando un grado en el caso de falsear la identidad).

C) Regla de extraterritorialidad

El artículo 367 quinquies establece:

> Las conductas de comercialización, distribución, difusión y exhibición, señaladas en el artículo anterior, se entenderán cometidas en Chile cuando se realicen a través de un sistema de telecomunicaciones al que se tenga acceso desde territorio nacional.

La ley deroga el antiguo artículo 374 ter, trasladando la regla de extraterritorialidad contenida en dicha norma, respecto a las conductas de comercialización, distribución y exhibición de material pornográfico, a un nuevo artículo 367 quinquies. Un aspecto interesante de la modificación es que incluye expresamente la *difusión* de material, que había sido omitida en la formulación original de la norma. Esto adquiere importancia dado que la mayoría de la doctrina y jurisprudencia ha indicado que justamente esta es la conducta que se lleva a cabo al enviar o mostrar material a través de Internet, aplicaciones u otras plataformas (por ejemplo, a través de programas *peer-to-peer*).[129]

c. captación, grabación y difusión de registros audiovisuales de los genitales u otra parte íntima del cuerpo (artículo 161-c inciso primero cp)

Este delito está contemplado en el artículo 161 C del Código Penal:

> Se castigará con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, al que en lugares públicos o de libre acceso público y que por cualquier medio capte, grabe, filme o fotografíe imágenes, videos o cualquier registro audiovisual, de los genitales u otra parte íntima del cuerpo de otra persona con fines de significación sexual y sin su consentimiento.
>
> Se impondrá la misma pena de presidio menor en su grado mínimo y multa de diez a veinte unidades tributarias mensuales, al que difunda dichas imágenes, videos o registro audiovisual a que se refiere el inciso anterior. En caso de ser una misma la persona que los haya obtenido y divulgado, se aplicarán a esta, la pena de presidio menor en su grado mínimo a medio y multa de veinte a treinta unidades tributarias mensuales.

A) Conducta típica

Estas figuras penales fueron introducidas en el Código Penal por la Ley 21.153, publicada el 3 de mayo del 2019, conjuntamente con los delitos de acoso sexual callejero y de abuso sexual por sorpresa. En específico, el nuevo artículo 161 C establece un listado alternativo de conductas destinadas a la captación o grabación de imágenes o video por cualquier medio.

129 Informe de la Comisión de Constitución, págs. 37 y sgts.

Las conductas sancionadas pueden clasificarse en dos grupos:

a) La mera captación, que implica recibir o recoger imágenes o video (por ejemplo, a través de cámaras que transmitan en vivo).
b) La grabación (incluyendo la filmación o fotografía), que apunta al almacenamiento de estas imágenes o video en algún tipo de soporte.

En el caso de la captación de imágenes o video, se está ante un delito de mera actividad, mientras que la grabación trae aparejado un resultado, consistente en la elaboración de un registro audiovisual.

Por su parte, el objeto sobre el cual se ejerce la conducta típica son los genitales u otra parte íntima del cuerpo. Según la redacción de la norma, se sanciona, en primer término, la captación o grabación de los genitales de la víctima (vulva o pene y escroto, según sea el caso), con o sin vestimentas. En este último caso, se apuntaría a imágenes o videos que señalen directamente a estas zonas del cuerpo (por ejemplo, la grabación de la ropa interior de las mujeres por debajo de vestidos o faldas).

Por su parte, se incluye en el tipo la frase «u otra parte íntima del cuerpo», en la que cabrían otras zonas corporales, distintas a los genitales, que dentro del medio social se mantienen generalmente cubiertas (por ejemplo, pechos o glúteos, también con o sin vestimentas).

Se requiere, por otra parte, la ausencia del consentimiento de la víctima. La conducta debe realizarse sin el consentimiento de la víctima; en caso contrario, será atípica. Respecto a este punto, para que la conducta sea atípica la persona ofendida debe autorizar expresamente la captación o grabación de sus genitales o de otra zona íntima de su cuerpo. Por ejemplo, debe estimarse sin consentimiento de la víctima si esta asintió a ser fotografiada de cuerpo entero y la otra persona grabó solo su zona genital.

El tipo exige también un elemento accidental relacionado con el espacio físico en el cual debe ejecutarse la conducta. Estos son lugares públicos o de libre acceso público, por ejemplo, calles, caminos, plazas, playas, establecimientos comerciales, restaurantes, servicentros, discotecas o lugares donde se desarrollen conciertos musicales, medios de transporte, etc. La captación o grabación en lugares privados sin el consentimiento de la víctima podría subsumirse en el actual artículo 161-A.[130]

130 Historia de la Ley, pág. 122, disponible en. https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8098/

B) Aspecto subjetivo

Hay aquí la exigencia de una finalidad determinada: con fines de significación sexual. Estamos en una situación similar a la del delito de abuso sexual con contacto, definido en el artículo 366 ter del Código Penal.[131]

C) Penalidad

La pena de este ilícito es presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales.

d. difusión de registros audiovisuales (artículo 161 c incisos segundo y tercero)

Se revisará cada aspecto relevante por separado.

A) Conducta típica

Difundir, por cualquier medio, los registros audiovisuales de los genitales u otra parte íntima del cuerpo de la víctima, obtenidos sin su consentimiento en lugares públicos o de libre acceso público.

B) Penalidad

En este caso, la pena es de presidio menor en su grado mínimo y multa de diez a veinte unidades tributarias mensuales. El aumento de la sanción respecto a la pena de multa se justifica por la mayor afectación a los bienes jurídicos, al poner en circulación los registros audiovisuales para que sean conocidos por terceras personas. En relación con este punto, basta con que el sujeto activo haya puesto a disposición del público las imágenes o videos (por ejemplo, a través de reproducción en vivo, redes sociales o sistemas de mensajería instantánea), sin que se requiera para la configuración del tipo penal que personas específicas hayan visto el material.

No es posible castigar a este título la difusión de registros audiovisuales captados con el consentimiento de la víctima (por ejemplo, fotografías o videos grabados en el contexto de una relación de pareja que hayan sido divulgados por redes sociales o en páginas web).

131 Respecto al concepto de significación sexual, se pronuncian a favor de un parámetro objetivo Garrido Montt. *Derecho Penal Parte Especial.* (actualización Francisco Maldonado), pág. 315 y Rodriguez Collao. *Delitos Sexuales*. 2016. pág. 250

C) Relación concursal con el delito de producción y difusión de material pornográfico en que hayan sido utilizados niños, niñas y adolescentes (artículos 366 quinquies y 374 bis).

Ante la captación, grabación o difusión de registros audiovisuales de los genitales de niños, niñas y adolescentes, deben apreciarse las figuras de producción y difusión de material pornográfico, contempladas en los artículos 366 quinquies y 374 bis del Código Penal, respectivamente, por un criterio de especialidad y dada la mayor penalidad asignada a estos delitos.

D) Referencias jurisprudenciales

Si bien están referidos al tipo penal establecido al artículo 161 A, previo a la incorporación de una tipificación más específica en esta letra C y a la actual letra podemos encontrar, a nivel jurisprudencial, una descripción de los verbos rectores de este delito, exigencias probatorias y referencia a la captación y grabación de imágenes del cuerpo humano:

- RIT 1218-2020, Juzgado de Garantía de Rengo, de 25 de mayo de 2022:

  Noveno: «El tipo penal exige en consecuencia que, mediante cualquier medio se capte, grabe, filme o fotografíe imágenes o hechos de carácter privado; que estos se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público; sin que exista autorización del afectado, ni de la ley, ni autoridad judicial alguna. En el caso tenemos que el imputado utilizando un teléfono celular grabó o al menos captó la imagen de la víctima en momentos que esta se vestía en su dormitorio, es decir, se cumplen todas las exigencias del tipo penal, primero y tal como ya se ha referido, utilizando un medio idóneo, como lo es un teléfono celular, captó imágenes de la víctima, mientras esta se vestía para salir a su trabajo, encontrándose desprovista de ropa en su parte superior, es decir, capturó un acto de absoluta intimidad, como lo es vestirse o desvestirse».

- RIT 298-2020, Tribunal de Juicio Oral en lo Penal de Iquique, de 13 de febrero de 2021:

  Décimo tercero: «Al analizar la norma en comento, se puede estimar que aquella busca proteger jurídicamente la vida privada de las personas, o 'intimidad', refiriéndose a un atentado a la libertad de mantener un espacio privado y, por ello, exclusivo, siendo un

reducto o área donde cada persona demuestra su opción de vida en forma diferente, garantizando la autonomía individual.

El tipo aplicable al caso de marras, presenta como verbos rectores el captar, que en una de sus acepciones implica 'Recibir, recoger sonidos, imágenes, ondas, emisiones radiodifundidas'; grabar, que a su vez concibe el 'captar y almacenar imágenes o sonidos por medio de un disco, una cinta magnética u otro procedimiento, de manera que se puedan reproducir', filmar que comprende 'Registrar imágenes en una película cinematográfica' o fotografiar 'Hacer una fotografía de alguien o algo', siendo la fotografía un 'Procedimiento o técnica que permite obtener imágenes fijas de la realidad mediante la acción de la luz sobre una superficie sensible o sobre un sensor'».

- Rol 32691-2018, Corte Suprema, de 29 de enero de 2019:

  Décimo segundo: «Que, las reflexiones anteriores, a diferencia de lo postulado en la sentencia impugnada, no importan exigir que se presente en el juicio como prueba el video que supuestamente habría grabado el acusado, ya que el mismo pudo haber sido borrado con posterioridad, sino únicamente que la sentencia exponga, sujetándose a las exigencias de los artículos 297 y 342 letra c) del Código Procesal Penal, de qué manera establece su existencia».

3.4 Delitos constitutivos de violencia de género digital

La violencia digital de género en contra de las mujeres y las niñas se desarrolla en un espacio en el que, si bien todos y todas nos desenvolvemos, continúa siendo incomprensible para la mayoría de las personas. No existen aún definiciones, conceptualizaciones y acuerdos respecto a cómo deben denominarse y/o clasificarse las conductas constitutivas de este tipo de violencia.

El Comité de Expertas (CEVI) del Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI), ante la ausencia de un acuerdo internacional en torno a la terminología adecuada para denominar esta forma de violencia, en su Informe sobre Ciberviolencia y Ciberacoso contra las mujeres y niñas en el marco de la convención Belém do Pará, 2022, utiliza indistintamente las expresiones «violencia facilitada por las TIC», «violencia en línea contra las mujeres», «violencia digital» y «ciberviolencia contra las mujeres», no obstante reconocer que la ex-

presión «violencia contra las mujeres facilitada por la tecnología de la información y las comunicaciones (TIC)» es quizás la más precisa, porque abarca la vasta gama de conductas que esta forma de violencia puede adoptar.[132]

La violencia digital tiene la particularidad de que no solo afecta la integridad física, psicológica y sexual de las mujeres, sino que además provoca su exclusión del espacio virtual. Incluso, en algunos casos, es esta exclusión el real objetivo de la violencia ejercida a través de medios digitales. Muchas mujeres y niñas, luego de vivir ataques a través de las redes sociales, las abandonan a veces por temor y otras por vergüenza o por ambas. Es decir, los sentimientos y el daño que una mujer o niña siente cuando es vulnerada o agredida en el espacio físico son comparables a los que experimenta cuando esta agresión se produce en el espacio virtual.

La sensación de humillación, vergüenza, impotencia, vulnerabilidad, etc., que una mujer o niña siente cuando es víctima de un acoso callejero es la misma que cuando recibe imágenes y contenido de carácter sexual, de forma repentina y no consentida, en sus dispositivos.

Comprender la magnitud del daño que puede producir la violencia digital solo es posible en la medida en que entendamos que cada vez en mayor medida las personas construyen sus identidades desde sus interrelaciones en Internet.

El estudio «Chile y la violencia de género en Internet» arrojó que las violencias digitales más vividas por mujeres en el país son acoso digital, usurpación de identidad, difamación, amenazas, pérdida de acceso a sus cuentas y envío de imágenes sexuales sin consentimiento.[133]

Hasta el 14 de junio del 2024, fecha en que se publica la ley N°21.675, que estatuye medidas para Prevenir, Sancionar y Erradicar la violencia en contra las Mujeres, en razón de su Género[134], no existía una tipificación específica de la violencia digital. Sin perjuicio de lo anterior

132 ONU Mujeres (2022), p. 9. Disponible en https://www.oas.org/es/mesecvi/docs/MESECVI-Ciberviolencia-ES.pdf.

133 ONG Amaranta *et al.* (2020), s.p. Disponible en https://amarantas.org/wp-content/uploads/2020/08/informe-proyecto-aurora.pdf.

134 Ley N° 21.675, que estatuye medidas para Prevenir, Sancionar y Erradicar la violencia en contra las Mujeres, debido a su Género. Esta ley unifica el concepto legal de las distintas violencias de las que pueden ser sujetos las mujeres, incluida la violencia digital, en un nuevo artículo 161 D del código Penal.

considerando los bienes jurídicos protegidos y las obligaciones que ha asumido el Estado de Chile al suscribir la Convención Belem do Pará, para prevenir, sancionar y erradicar la violencia contra la mujer, muchas formas de violencia digital era posible encuadrarlas en nuevas formas de comisión de figuras típicas, como el delito de amenazas de los artículos 296 y 297; el ya mencionado artículo 161 C; la obtención de información, como por ejemplo fotografías de la víctima, a través del acceso ilegítimo a un sistema informático, el sancionado en el artículo 2° de la Ley 21.459, etc.

Por último, es en la violencia de pareja donde se han evidenciado con mayor intensidad las manifestaciones de violencia digital. En estas relaciones, la convivencia permanente o temporal en un mismo espacio físico facilita el control del espacio digital, generalmente de las mujeres. La introducción de *software* inteligente para hacer seguimientos o acceder a los dispositivos y/o plataformas virtuales es la nueva modalidad a través de las cuales se ejecuta el delito de maltrato habitual del artículo 14 de la Ley 20.066.

A modo de construcción jurisprudencial de la tipificación de hechos constitutivos de violencia digital de género, destaca la siguiente resolución del Juzgado de Garantía de Valdivia, dictada con fecha 25 de noviembre de 2022, en caso seguido por delito de injurias graves por escrito con publicidad, previsto y sancionado en los artículos 416 y 417 números 3, 4, 5, en relación con el 418 del Código Penal.

En este fallo, RIT 143-2022, el tribunal consigna en su considerando noveno:

> […] cuando existen acciones tendientes a invadir la intimidad, más aún, como se ha acreditado en autos, provocan en la víctima una deshonra constante, traduciéndose en información vertida por el imputado que, no autorizado ni ha ratificado la víctima, dichos no consentido por la destinataria, atentando contra su dignidad y la privacidad, en lo que a su intimidad se refiere.
>
> […] a pesar de lo que indica la defensa, en el sentido que, el ánimo del imputado es solo buscar la verdad, de la paternidad de la niña, latamente mencionada, toda la prueba incorporada, el enfoque de género permite visualizar, que la víctima, es una persona que ha estado expuesta a estas acciones, que se traducen en definitiva que la querellante vea mermada sustancialmente su derecho a una vida libre de violencia, tanto en el ámbito público como en el privado […].

Y en el considerando décimo expone que «[…] el titular del derecho a la propia imagen mantiene privacidad y control sobre la misma, y además protección sobre dicha imagen lo que tiene especial importancia en la actualidad, dado el creciente desarrollo de TIC y procedimientos que posibilitan enormemente la captación y difusión de imágenes e información de las personas».

Nuevo Delito constitutivo de Violencia de Genero Digital, Exhibición y difusión de contenido sexual sin consentimiento.

Con fecha 14 de junio del 2024, se publicó la Ley N° 21.675, que estatuye medidas para Prevenir, Sancionar y Erradicar la violencia en contra las Mujeres, debido a su Género. Esta ley, además de establecer medidas en distintos ámbitos, unifica el concepto legal de las distintas violencias de las que pueden ser sujetos las mujeres.

Para los efectos de poder determinar cuándo podríamos estar en presencia de conductas constitutivas de violencia digital de género, resultan especialmente relevante los siguientes artículos de la Ley N° 21.675:

> **Artículo 5.-** *Definición de violencia de género.* ***Es violencia de género*** *cualquier acción u omisión que cause muerte, daño o sufrimiento a la mujer en razón de su género, donde quiera que ocurra, ya sea en el ámbito público o privado; o una amenaza de ello.*
>
> *También será considerada violencia de género aquella ejercida contra niñas, niños y adolescentes, con el objeto de dañar a sus madres o cuidadoras. En estos casos, las personas menores de 18 años de edad serán derivadas al órgano competente conforme a lo dispuesto en la ley N°21.430, sobre Garantías y Protección Integral de los Derechos de la Niñez y Adolescencia.*
>
> *La omisión en la observancia de los deberes que por esta ley corresponden a los órganos del Estado y sus agentes, habilita para interponer las acciones administrativas y judiciales, según correspondan, ante el órgano respectivo, con el fin de restaurar el ejercicio y goce de tales derechos, a través de los recursos y procedimientos contemplados en las leyes.*

> **Artículo 6.-** *Formas de violencia de género. La violencia en contra de las mujeres en razón de su género incluye, entre otras, las siguientes:*
>
> **2.** *Violencia psicológica: toda acción u omisión, cualquiera sea el medio empleado, que vulnere, perturbe o amenace la integridad psíquica, tales como tratos humillantes, vejatorios o degradantes, control o vigilancia de*

conductas, intimidación, coacción, sumisión, aislamiento, explotación o limitación de la libertad de acción, opinión o pensamiento.

3. *Violencia sexual: toda conducta que vulnere, perturbe o amenace la libertad, integridad y autonomía sexual y reproductiva de la mujer; y su indemnidad en el caso de las niñas.*

5. *Violencia simbólica: toda comunicación o difusión de mensajes, textos, sonidos o imágenes en cualquier medio de comunicación o plataforma, cuyo objeto sea naturalizar estereotipos que afecten su dignidad, justificar o naturalizar relaciones de subordinación, desigualdad o discriminación contra la mujer que le produzcan afectación o menoscabo.*

Asimismo, junto con modificar diversos cuerpos legales, incorpora en el Código Penal un nuevo delito, agregando una letra D al art. 161. Esta figura, por un parte, atiende expresamente a cubrir un espacio de impunidad respecto de conductas que no quedaban claramente cubiertas en las letras A y C del art. 161 del Código Penal y, por otra, armonizan esta ley con el proyecto de ley que tipifica y sanciona la violencia digital[135], y otorga protección a las víctimas.

Exhibición y difusión de contenido sexual sin consentimiento.

Artículo 161-D.- *El que sin autorización expresa exhibiere registro de imágenes o sonidos en que se representa una acción sexual que involucra a otro o imágenes íntimas de connotación sexual, independiente de como haya sido obtenido, será sancionado con la pena de prisión y multa de cinco a diez unidades tributarias mensuales.*

En caso de envío, difusión o publicación de dicho registro, se impondrá la pena de presidio menor en su grado mínimo y multa de once a veinte unidades tributarias mensuales.

A) Conducta Típica

Las conductas sancionadas pueden ser alternativa e indistintamente:

a) Inciso primero: Exhibición de registros: Entendiéndose por tal el "manifestar, mostrar en público"[136], registros de sonidos e imágenes, sin autorización expresa de quién participa de esa representación sexual.

135 Boletín N°13928-07. Disponible en https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8303/.

136 Definición RAE, *vigésima segunda edición (2001)*

El verbo "exhibir", debe entenderse en los mismos términos en que ha sido utilizado por el legislador en los delitos de abuso sexual sin contacto, art. 366 quáter y en el de comercialización, importación, exportación, distribución, difusión y exhibición de material pornográfico o de explotación sexual de personas menores de dieciocho años del artículo 367 quáter, ambos del Código Penal. De acuerdo con la RAE, exhibir es manifestar, mostrar en público o a otras personas. En consecuencia, puede referirse tanto a la exhibición de una fotografía en soporte material, a la proyección de un video o imagen fotografiada, en cualquier dispositivo, celular, computador, Tablet, etc.

En el caso de estos registros de sonidos o imágenes de representación sexual, basta para configurar la conducta que el autor le muestre el material a un tercero, por ejemplo, en su celular o dispositivo electrónico, sin autorización expresa.

El ejemplo que más se menciona, debido a su alta frecuencia, es la exhibición de una fotografía o video tomada o grabada por una mujer, o bien, con su consentimiento, la que envía a su pareja o a cualquier persona, pero con una mínima expectativa de privacidad y el destinatario de la imagen la muestra a otras personas.

b) **Inciso segundo: Enviar, difundir y publicar dichos registros:** Estas tres conductas están referidas al hecho de compartir con otras personas, más allá de la exhibición, los sonidos o registros de una representación sexual, no autorizado por quién es parte de esta representación. Es decir, el autor, saca de su esfera de resguardo estos registros y los pone en circulación. Si este envío, difusión o publicación de estos registros se realiza a través de medios tecnológicos o digitales, mediante la transferencia de los archivos, de un sistema informático a otro, o se publica en redes o portales sociales, como Telegram, WhatsApp, Onlyfans, o Arsmate, etc., lo que necesariamente implica su propagación, constituye Violencia Digital.

En este último caso el legislador estimó que la difusión de los registros es de mayor lesividad, por lo que la pena privativa de libertad es de simple delito.

Es importante recalcar que la falta de **consentimiento expreso** es un elemento del tipo penal.

B) Bien Jurídico Protegido.

Si bien este delito no exige un sujeto pasivo especial, es importante tener presente que ha sido establecido en la Ley Integral para Prevenir, Sancionar y Erradicar la Violencia en contra de las Mujeres, por lo tanto, es un delito pluriofensivo, en este sentido pretende proteger la **privacidad e intimidad** de las personas; la legitima expectativa de privacidad de una persona que autoriza a que otra capte o grabe su imagen o los sonidos que emite (o los registra ella misma) a que estos registros no se exhiban, envíen, difundan o publiquen a terceros, sin su expreso consentimiento y, el derecho de las mujeres a vivir una vida libre de violencia, incluida la sicológica y simbólica.

C) Concursos.

a.- Delito de producción y difusión de material pornográfico en que hayan sido utilizados niños, niñas y adolescentes (artículos 366 quinquies y 374 bis).

Ante la captación, grabación o difusión de registros audiovisuales de los genitales de niños, niñas y adolescentes, en nuestra opinión deben preferirse las figuras de producción y difusión de material pornográfico, contempladas en los artículos 366 quinquies y 374 bis del Código Penal, respectivamente, por un criterio de especialidad y dada la mayor penalidad asignada a estos delitos.

b.- Delitos contra la intimidad de los artículos 161-A y 161-C.

Estos delitos no contemplan la exhibición, por lo tanto, si la captación o grabación de imágenes o sonidos fue realizada sin autorización o consentimiento y, dependiendo del lugar donde se hayan obtenido (de libre acceso público o no), deberán ser sancionadas de acuerdo con los arts. 161 A o C. Si, además, hay exhibición de estas imágenes o sonidos tipificadas en nuevo art. 161 D, estaremos en presencia de un concurso real de delitos que deberían sancionarse de manera independiente o acumulativa.

Por el contrario, si estamos ante la figura del art. 161 D inc. 2°, es decir conductas de difusión, publicación o envío, estaríamos ante un concurso ideal de delitos respecto de las figuras de los arts. 161 A y C, en que el criterio para preferir entre unas y otras, estará determinado, en nuestra opinión, por la naturaleza del contenido de las imágenes o sonidos y por la ausencia o no, de autorización o consentimiento de la víctima en la obtención de los registros[137].

137 Primer Informe de la Comisión Especial encargada de conocer iniciativas y tramitar proyectos de ley relacionados con la mujer y la igualdad de género, p.40.

4. Circunstancias modificatorias de responsabilidad penal

Otra de las novedades que introdujo la LDI es la incorporación de nuevas circunstancias modificatorias de responsabilidad penal aplicables para los delitos contemplados en este cuerpo legal, como son, por un lado, la circunstancia atenuante de la colaboración eficaz, también denominada en otras leyes como delación compensada, y que se enmarca dentro de lo que la doctrina denomina el derecho penal premial; y, por otro, las circunstancias agravantes del artículo 10, donde se pueden identificar dos agravantes comunes, relacionadas con abusos de posición o de una situación de vulnerabilidad de un tercero, y una agravante especial o calificada, que dice relación con determinados daños causados por el delito y que se establecen expresamente.

4.1. Colaboración eficaz

Como se dijo, la Ley 21.459, en su origen, regulaba expresamente la atenuante de cooperación eficaz, ampliando con ello el grupo de delitos que la contemplaban expresamente, tales como los establecidos en la Ley 20.000, la Ley 19.913, el Decreto Ley 211 o en el Título V del Libro II del Código Penal, todo lo cual fue recientemente modificado por la Ley 21.694 que "Modifica los cuerpos legales que indica para mejorar la persecución penal en materia de reincidencia y delitos de mayor connotación social", de 4 de septiembre de 2024, que introdujo el Párrafo 4° bis al Título I del Libro II del Código Procesal Penal denominado «De la cooperación eficaz con la investigación», regulando de forma más genérica esta minorante respecto de varias categorías delictivas que para el legislador han merecido, en la actualidad, un tratamiento diferenciado y de consecuencias mayormente categóricas, entre las que ha considerado los delitos informáticos de la Ley 21.459.

Para hablar de la institución de la colaboración eficaz, sea en su regulación actual o en la primitiva de la Ley 21.459 es necesario situarla dentro de un fenómeno mayor, el del derecho penal premial, que consiste en otorgar beneficios por el arrepentimiento de una persona que ha cometido un delito. Esta figura representa una forma *sui generis* de des-

---

Intervención de la profesora Myrna Villegas Díaz. Disponible en https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8303/

penalización, ya que se pretende incentivar o premiar a aquel individuo que colabora con la administración de justicia, por lo general a través de una reducción o exención de pena.[138]

En este sentido, el premio, generalmente materializado a través de un beneficio penológico, es usado como una herramienta de fomento de ciertas conductas –en este caso, de la colaboración con la investigación penal–, lo cual representa un cambio importante en la forma de entender al derecho penal como un instrumento de control social, desde una legislación punitiva que busca desincentivar ciertas conductas a través de la amenaza de un castigo (la pena) a una que alienta ciertas conductas, consideradas ventajosas.[139]

El fundamento habitual para justificar la implementación de mecanismos de derecho penal premial suele ser la necesidad de otorgar nuevas herramientas investigativas a los sistemas de persecución criminal, en atención al aumento acelerado de la delincuencia organizada y la aparente incapacidad de la institucionalidad actual de hacer frente a esta amenaza. En este sentido, puede descartarse que la justificación de la colaboración eficaz como eximente o atenuante de la responsabilidad penal tenga algo que ver con la posición anímica del delincuente respecto al delito que cometió, siendo del todo irrelevante si su arrepentimiento es genuino o no.[140]

Para ilustrar lo recién señalado, basta ver la redacción del derogado artículo 9° de la Ley 21.459[141] o la regulación actual de la cooperación eficaz en el Código Procesal Penal, pudiendo colegirse, en ambos casos, que el legislador no realiza ninguna exigencia de tipo subjetivo al imputado que quiera acogerse a este beneficio, sino tan solo que su colaboración sea considerada eficaz a juicio del Ministerio Público, por regla general.

En principio, conforme al texto no vigente de la Ley 21.459 la concurrencia de la atenuante debía ser expresada por el fiscal en la formalización de la investigación o en el escrito de acusación. En la actualidad, la cooperación eficaz puede concurrir sobre la base de tres modalidades distintas: (1) por un acuerdo de cooperación eficaz entre fiscal e imputa-

138 Arenas (2022), p. 5.
139 *Ídem.*
140 *Ídem.*
141 *Ídem.*

do, el que incluso puede llegar a ser muy calificado (2) el reconocimiento de la atenuante por el fiscal, sin acuerdo, y (3) por el reconocimiento que hace el tribunal, aunque la modificatoria no haya sido invocada por el fiscal, en la medida que, durante el juicio, haya quedado acreditado que el imputado cooperó con la investigación.

La ley define la cooperación eficaz de la misma forma que lo hacía la Ley 21.459 y que corresponde a otras regulaciones de esta atenuante, cuando se establecía separadamente por categorías de delito y corresponde al *"(…) suministro de datos o informaciones precisas, verídicas y comprobables que contribuyan al esclarecimiento de los hechos investigados o permitan la identificación de sus responsables, o sirvan para prevenir o impedir la perpetración, la continuidad o la reiteración de otros delitos, o faciliten la práctica de cualquier clase de comiso"*[142].

A su vez, es posible que sea llevada a cabo a través de diversos medios, toda vez que el legislador no establece mecanismos específicos para el esclarecimiento de los hechos. Por ende, será posible proporcionar informaciones orientadas a esa finalidad mediante declaraciones verbales; documentos, incluidos los electrónicos; archivos de audio o video, o programas computacionales.[143] Sin embargo es preciso considerar que, en la regulación vigente, las condiciones o el contenido básico que debe cumplir la información entregada es algo que forma parte del acuerdo.

Además, la información suministrada por alguna de las vías señaladas u otras que sean idóneas ha de ser precisa, verídica y comprobable. La precisión excluye datos ambiguos o vagos, que no permitan a los persecutores el desarrollo de líneas investigativas para el esclarecimiento de delitos de igual o mayor gravedad. Que la información sea verídica significa que los datos proporcionados deben corresponderse con la realidad; por lo tanto, resulta necesario que efectivamente existan otros hechos y otros partícipes en delitos informáticos. Finalmente, el carácter comprobable ha sido interpretado en el sentido de que el desarrollo de la investigación, por parte del Ministerio Público y de las policías, a partir de la información proporcionada, permita efectivamente descubrir otros hechos constitutivos de delito y establecer la participación de sus responsables.[144]

142 Artículo 228 bis A inciso primero del CPP.
143 Mayer y Vera (2022b), p. 307.
144 *Ídem.*

En cuanto a su efecto penológico, considerando la regulación ampliada que actualmente se hace de esta atenuante, se advierten consecuencias jurídicas abultadas en relación a la regulación anterior. En efecto, con la atenuante específica del artículo 9° de la Ley 21.459 el imputado aspiraba a un régimen más moderado que lo que se establecía en otros cuerpos legales, ya que el juez solo podía reducir la pena en un grado, lo cual difería de otras leyes, como la Ley 20.000, donde la pena podía reducirse hasta en tres grados. El texto vigente, en cambio, contempla la posibilidad de rebaja hasta en dos grados de la pena, cuando se trate de un acuerdo de cooperación eficaz simple, y hasta en tres grados e, incluso, el sobreseimiento definitivo, cuando se trate de un acuerdo de cooperación eficaz calificada, vale decir, se trate de aquélla que permita la consecución de fines tan importantes para el combate contra el crimen organizado como la identificación de los líderes de una organización delictiva, de sus bienes o permitan conocer la ubicación de víctimas de delitos graves como el secuestro o la trata de personas, entre otros.

Con la redacción anterior, que le exigía al fiscal que mencionara expresamente si la cooperación prestada por el imputado había conducido al esclarecimiento de hechos investigados que fueran constitutivos de alguno de los delitos informáticos, a la identificación de sus responsables o había servido para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad contemplados en la misma LDI, cierta doctrina entendía que era el órgano persecutor penal el que determinaba la concurrencia de la atenuante, razón por la cual ella solo era aplicable si así lo establecía el Ministerio Público.[145]

Sin embargo, en opinión de Mayer y Vera, el pronunciamiento final en torno a la concurrencia de esta circunstancia debía quedar entregado a los tribunales de justicia, incluso en el evento en que no fuera reconocida por el Ministerio Público, por cuanto la apreciación de circunstancias modificatorias integra la fase de juzgamiento penal, función que no corresponde en caso alguno al órgano persecutor, por disponerlo expresamente el artículo 83 inciso primero de la Constitución Política de la República. En ese orden de ideas, si, por ejemplo, el imputado prestaba declaración, aportando datos que cumplían con todos los requisitos establecidos en la ley y el Ministerio Público no reconocía la atenuante, por entender que la información no es comprobable, el abogado defen-

145 Silva (2011), p. 223.

sor podía, en cualquier caso, intentar demostrar su pertinencia en el respectivo procedimiento o juicio.[146]

Esa discusión se encuentra superada con la nueva redacción de la minorante que dispone expresamente, en el artículo 228 bis A inciso 4° del CPP, que el acuerdo de cooperación eficaz resulta vinculante para el tribunal, con la sola exigencia de que éste sea procedente conforme a la categoría de delitos de que se trate. Por otro lado, la regulación general concluye señalando que el tribunal puede perfectamente reconocer la cooperación eficaz, aunque ésta no haya sido invocada por el Ministerio Público cuando, durante el juicio, haya quedado acreditado que el imputado colaboró con la investigación.

4.2. Circunstancias agravantes

El artículo 10 de la LDI consagra lo siguiente:

> Constituyen circunstancias agravantes de los delitos de que trata esta ley:
> 1) Cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función.
> 2) Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.
>
> Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la Ley Nº 18.700, orgánica constitucional sobre votaciones populares y escrutinios, la pena correspondiente se aumentará en un grado.

La primera de las agravantes especiales introducidas por la Ley de Delitos Informáticos se denomina de abuso de confianza, y presupone una especial posición por parte del sujeto activo del delito, quien debe ejecutarlo en razón del ejercicio de un cargo o función. Implica, por tanto, que exista una confianza depositada en quien tiene a su cargo la administración de un sistema informático o la custodia de los datos informáticos ahí contenidos, y que este abuse de aquella para cometer el delito.

146 Mayer y Vera (2022b), p. 307.

En el contexto de la delincuencia informática, es común que se refiera la actuación de «insiders», que corresponden a «trabajadores o prestadores de servicios de la empresa o establecimiento afectado» que se encuentran en una posición especialmente ventajosa para la comisión de la conducta delictiva, derivada de su vínculo con la víctima. Tal forma de operar se opone a los ataques informáticos que provienen, por así decirlo, del exterior, por parte de un sujeto que carece de la relación indicada.[147]

Existe una clara similitud entre esta agravante y aquella prevista en el artículo 12 número 7 del Código Penal, «cometer el delito con abuso de confianza». Debido a que ambas circunstancias tienen el mismo fundamento político-criminal, es decir, sancionan con mayor gravedad a quien cometa el delito desde una posición que aumente la indefensión de la víctima, no es posible aplicarlas simultáneamente sin infringir el principio del *non bis in idem*, existiendo más bien una relación de género a especie entre una y otra.

La segunda de las agravantes comunes de la Ley 21.459 corresponde a una agravante de vulnerabilidad, cuyo fundamento radica en el estado de indefensión en que se encuentran las personas indicadas por la norma, esto es, niños, niñas, adolescentes y adultos mayores. Cabe mencionar que el simple hecho de ser la víctima del delito alguna de las personas referidas no implica automáticamente la aplicación de la agravante, siendo necesario probar que existió efectivamente un abuso de su vulnerabilidad, confianza o desconocimiento.

La regulación de esta agravante puede entenderse como expresión de una tendencia en orden a ampliar la aplicación de la circunstancia modificatoria de alevosía a ámbitos distintos de los delitos contra las personas. Recordemos que esta última agravante, regulada en el artículo 12 número 1 CP, establece explícitamente que constituye una circunstancia que determina una agravación del castigo el hecho de «cometer el delito contra las personas con alevosía, entendiéndose que la hay cuando se obra a traición o sobre seguro». En ese sentido, el legislador ha ido extendiendo el ámbito de procedencia de dicha agravante, por ejemplo, a algunos de los delitos sexuales, cuestión que ha requerido de reformas legales expresas, por tratarse de contextos en los que la agravante genérica no resultaría aplicable.[148]

147 *Ídem.*
148 *Ídem.*

Al igual que en el caso de la agravante del numeral 1 del artículo 10, el fundamento político-criminal es la indefensión de la víctima, dada la posición de riesgo en que se encuentra, que, en el caso del abuso de confianza, viene dada por la especial posición del sujeto activo y, en el caso del numeral segundo, por la especial situación de vulnerabilidad de la víctima. Esto trae como consecuencia que no pueden ser aplicadas conjuntamente, ni tampoco acompañadas del abuso de confianza del artículo 12 número 7 del Código Penal ni de la agravante genérica de alevosía, así como de ninguna otra agravante que tenga el mismo fundamento político-criminal.

Finalmente, la nueva ley contempla la agravante de infraestructura crítica, según la cual «si como resultado de la comisión de las conductas contempladas en este título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la Ley Nº 18.700, orgánica constitucional sobre votaciones populares y escrutinios, la pena correspondiente se aumentará en un grado». Cabe precisar que se hace referencia a las conductas contempladas en el Título I de la LDI.

El fundamento de la agravante en comento radica en el mayor injusto implicado en conductas que impactan negativamente en infraestructura crítica. Por ende, lo que está en juego es una posible afectación, de gran entidad y particularmente intensa, de los bienes jurídicos asociados a la infraestructura que resulta impactada a través de la comisión de delitos informáticos.[149] Para evitar discusiones en torno a lo que debe entenderse por infraestructura crítica, el legislador rechazó dar una definición de aquella y, en cambio, determinó un listado de servicios que pueden incluirse dentro de aquel concepto. Esta enumeración no es taxativa, e incluye la afectación e interrupción de la provisión o prestación de servicios de utilidad pública, o bien del normal desenvolvimiento de los procesos electorales.

La ley exige que «[…] si como resultado de la comisión de las conductas contempladas en este Título, se afectase o se interrumpiese […]», es decir, debe existir una relación de causalidad suficientemente acreditada entre el delito y la afectación a la infraestructura crítica.

149 *Ídem.*

Por último, desde un punto de vista penológico, esta corresponde a una agravante especial o calificada, ya que su efecto agravador es más intenso que el de una agravante común (permite aumentar en un grado la pena asignada al delito). Al igual que sucedía con la atenuante de la colaboración eficaz del artículo 9°, esta agravante no debe ser ponderada racionalmente con las otras circunstancias modificatorias y deberá ser aplicada en todo caso.

4.3. Circunstancias modificatorias previstas en la Ley de Delitos Económicos

En esta parte no podemos dejar de mencionar que el artículo 2° número 20 de la Ley 21.595 considera a todos los delitos de la LDI (artículos 1° a 8°) como delitos económicos de segunda categoría y les son aplicables las circunstancias modificatorias de responsabilidad penal que establece esta nueva legislación. Al ser este un trabajo sobre la criminalidad informática, excedería la finalidad del mismo desarrollar un análisis exhaustivo de las atenuantes y agravantes previstas en la Ley de Delitos Económicos, quedando esa labor reservada para eventuales trabajos similares sobre la criminalidad económica y las importantes modificaciones legales introducidas en el último tiempo.

Sin embargo, sí nos resulta necesario hacer a lo menos una mención a las circunstancias modificatorias previstas en la Ley 21.595, ya que se trata de normas que, probablemente, deberán primar en un caso concreto.[150]

Antes de entrar al detalle de cada una de ellas, es necesario hacer la prevención en cuanto a que los delitos de la LDI, como ya se dijo, son delitos económicos de segunda categoría y, por lo tanto, es necesario que sean perpetrados en ejercicio de un cargo, función o posición en una empresa, o en beneficio económico o de otra naturaleza para una empresa. En caso contrario, no les serán aplicables las disposiciones de esta ley.

150 El inciso segundo del artículo 9° de la Ley 21.595 señala que la pena privativa de libertad que se imponga será la que se determine conforme a esa misma ley y no por la de la ley que tipifica el delito, del modo siguiente: «*No obstante, la determinación de la pena de presidio o reclusión que deba ser impuesta, así como de su sustitución, se harán conforme con la presente ley. En subsidio serán aplicables las reglas generales de determinación y ejecución de las penas, en tanto no sean incompatibles con la presente ley*».

A) Atenuantes

El artículo 13 de la LDE señala que serán circunstancias atenuantes de un delito económico las siguientes:

1.ª La culpabilidad disminuida del condenado, establecida siempre que concurra cualquiera de los siguientes supuestos:
a) El condenado no buscó obtener provecho económico de la perpetración del hecho para sí o para un tercero.
b) El condenado, estando en una posición intermedia o superior al interior de una organización, se limitó a omitir la realización de alguna acción que habría impedido la perpetración del delito, sin favorecerla directamente.
2.ª Que el hecho haya ocasionado un perjuicio limitado. Se entenderá que ello tiene lugar cuando el perjuicio total supere las 40 unidades tributarias mensuales y no pase de 400, sin que se aplique lo dispuesto en el literal b) de la circunstancia 2.ª del artículo 16.

B) Atenuantes muy calificadas

Por su parte, el artículo 14 considera como atenuantes muy calificadas las siguientes:

1.ª La culpabilidad muy disminuida del condenado, establecida siempre que concurra cualquiera de los siguientes supuestos:
a) El condenado actuó en interés de personas necesitadas o por necesidad personal apremiante.
b) El condenado tomó oportuna y voluntariamente medidas orientadas a prevenir o mitigar sustancialmente la generación de daños a la víctima o a terceros.
c) El condenado actuó bajo presión y en una situación de subordinación al interior de una organización.
d) El condenado actuó en una situación de subordinación y con conocimiento limitado de la ilicitud de su actuar.
2.ª Que el hecho haya tenido una cuantía de bagatela. Se entenderá especialmente que ello es así, cuando:
a) El perjuicio total irrogado no supere 40 unidades tributarias mensuales.
b) Concurra cualquiera de las causales atenuantes señaladas en el inciso primero del artículo 111 del Código Tributario, respecto de

delitos económicos que constituyan infracción a las normas tributarias.

C) Agravantes

El artículo 15 consagra como circunstancias agravantes las siguientes:

1.ª La culpabilidad elevada del condenado, establecida siempre que concurra cualquiera de los siguientes supuestos:
   a) El condenado participó activamente en una posición intermedia en la organización en la que se perpetró el delito.
   En el caso de organizaciones privadas o de empresas o universidades del Estado, se entenderá que el condenado se encuentra en una posición intermedia cuando ejerce un poder relevante de mando sobre otros en la organización, sin estar en una posición jerárquica superior. Este supuesto no será aplicable tratándose de medianas empresas conforme al artículo segundo de la Ley N° 20.416.
   Tratándose de órganos del Estado, se entenderá que el condenado se encuentra en una posición intermedia cuando ejerce un poder relevante de mando sobre otros en la organización, sin estar en alguna de las situaciones previstas en el número 1° del artículo 251 quinquies del Código Penal, aunque no haya sido condenado por alguno de los delitos allí mencionados.
   b) El condenado ejerció abusivamente autoridad o poder al perpetrar el hecho.
   c) El condenado había sido sancionado anteriormente por perpetrar un delito económico.
   d) El condenado por delito económico constitutivo de infracción a las normas tributarias se encuentra en cualquiera de las situaciones señaladas por los incisos segundo y tercero del artículo 111 del Código Tributario.
2.ª Que el hecho haya ocasionado un perjuicio o reportado un beneficio relevante. Se entenderá que ello tiene lugar cuando el perjuicio o beneficio agregado total supere las 400 unidades tributarias mensuales y no supere las 40.000, sin que se aplique alguno de los casos de la circunstancia 2.ª del artículo 16.

D) Agravantes muy calificadas

Por último, el artículo 16 establece como agravantes muy calificadas las siguientes circunstancias:

1.ª La culpabilidad muy elevada del condenado, establecida siempre que concurra cualquiera de los siguientes supuestos:
   a) El condenado participó activamente en una posición jerárquica superior en la organización en la que se perpetró el delito.
   Tratándose de organizaciones privadas o de empresas o universidades del Estado, se entenderá que el condenado se encuentra en una posición jerárquica superior en la organización cuando ejerza como gerente general o miembro del órgano superior de administración, o como jefe de una unidad o división, solo subordinado al órgano superior de administración, así como cuando ejerza como director, socio administrador o accionista o socio con poder de influir en la administración.
   En el caso de los delitos a los que se refiere el artículo 1, esta agravante solo será aplicable respecto de quienes intervinieren en el hecho en ejercicio de un cargo, función o posición en una empresa cuyos ingresos anuales sean iguales o superiores a los de una mediana empresa conforme al artículo segundo de la Ley Nº 20.416, o cuando lo fuere en beneficio económico o de otra naturaleza de una empresa que tenga esa condición.
   Tratándose de organizaciones públicas, se entenderá que el condenado se encuentra en una posición jerárquica superior cuando se encontrare en alguna de las situaciones previstas en el número 1º del artículo 251 quinquies del Código Penal, aunque no haya sido condenado por alguno de los delitos allí mencionados.
   b) El condenado ejerció presión sobre sus subordinados en la organización para que colaboraran en la perpetración del delito.
2.ª Que el hecho haya ocasionado un perjuicio muy elevado. Se entenderá que ello tiene lugar en las siguientes circunstancias:
   a) Cuando el hecho haya ocasionado perjuicio a personas naturales o jurídicas, públicas o privadas, que en total supere las 40.000 unidades tributarias mensuales, o haya reportado un beneficio de esta cuantía.
   b) Cuando el hecho haya afectado el suministro de bienes de primera necesidad o de consumo masivo.

c) Cuando el hecho haya afectado abusivamente a individuos que pertenecen a un grupo vulnerable.
d) Cuando concurrieren las circunstancias previstas en el número 2° del artículo 251 quinquies o en el artículo 260 ter del Código Penal.

De concurrir alguna atenuante muy calificada o una agravante muy calificada, se estará a lo previsto en el artículo 17:

> Efectos de las atenuantes y agravantes. En caso de concurrir una atenuante muy calificada respecto de un marco penal que incluya una pena de presidio o reclusión de un solo grado, este se aplicará en su mínimum. De estar compuesto de dos o más grados, no se aplicará el grado superior.
>
> De concurrir dos o más atenuantes muy calificadas respecto de un delito cuyo marco esté compuesto por un solo grado, este se rebajará en un grado. De estar compuesto de dos o más grados, el marco se fijará en el grado inmediatamente inferior al grado más bajo del marco legal.
>
> En caso de concurrir una agravante muy calificada respecto de un marco penal que incluya una pena de presidio o reclusión de un solo grado, este se aplicará en su máximum. De estar compuesto de dos o más grados, no se aplicará el grado inferior.
>
> De concurrir dos o más agravantes muy calificadas respecto de un delito cuyo marco esté compuesto por un solo grado, este se incrementará en un grado. De estar compuesto de dos o más grados, el marco se fijará en el inmediatamente superior al grado más alto del marco legal.
>
> De concurrir atenuantes muy calificadas y agravantes muy calificadas, el tribunal deberá compensarlas en consideración a su número. En caso de que concurran en igual número, no producirán efecto de atenuar o agravar la pena.

5. Los delitos informáticos como base de responsabilidad penal de la persona jurídica

Coincidente con la importancia que se ha dado a las conductas ilícitas en el marco corporativo, y a su potencial impacto en el orden económico, la LDI incorpora los delitos informáticos tipificados en la misma como base de responsabilidad penal empresarial, lo cual ratifica la relevancia de esta categoría delictiva al interior del ordenamiento jurídico chileno.

A este respecto, cabe tener presente dos situaciones: una es la referida a la modificación que la LDI introdujo en la Ley 20.393, sobre Responsabilidad Penal de las Personas Jurídicas, y otra, la gran modificación que ha implicado la Ley 21.595, sobre Delitos Económicos, que, como se señaló, incorpora los delitos de la LDI en la segunda categoría de delitos económicos y, por ende, como base de responsabilidad penal de las personas jurídicas, cumpliéndose los presupuestos que contempla la ley modificada. En esta parte, la Ley 21.595 entró en vigencia el 1 de septiembre de 2024.

5.1. Delitos informáticos como base de responsabilidad penal de la persona jurídica en la actualidad (modificación de la Ley 21.459)

En la redacción anterior a la vigencia de la LDE, para que una persona jurídica tuviera responsabilidad penal era necesaria la concurrencia de los siguientes presupuestos:

a. Que se haya cometido un delito de la LDI por los dueños, controladores, responsables, ejecutivos principales, representantes o quienes realicen actividades de administración y supervisión dentro de la persona jurídica, o por personas naturales que estén bajo la dirección o supervisión directa de alguno de los sujetos mencionados.
b. Que ese delito se haya cometido en interés o provecho de la persona jurídica, si bien no se exige que sea un propósito exclusivo, sí debe estar presente este interés.
c. Que la comisión del delito sea consecuencia del incumplimiento, por parte de la persona jurídica, de sus deberes de dirección y supervisión, por lo que cobran importancia los modelos de prevención de delitos al interior de las organizaciones, cuyos elementos mínimos se contemplan en el artículo 4°.

5.2. Delitos informáticos como base de responsabilidad penal de la persona jurídica a partir del 1 de septiembre de 2024 (modificación de la Ley 21.595)

Con la Ley de Delitos Económicos se producen cambios sustanciales en materia de responsabilidad penal corporativa. Lo anterior es coheren-

te con el espíritu de dicha legislación, que viene a constituir un régimen más severo en materia de criminalidad económica que, al condicionar ciertas categorías de delitos a la existencia de un contexto corporativo, bien podríamos llamar criminalidad empresarial.

Por ello, y como se anticipó, el artículo 2° de la Ley 21.595 establece que se considerarán como delitos económicos los delitos tipificados en los artículos 1° a 8° de la LDI en la medida que sean cometidos por alguna persona dentro de la empresa, o en beneficio de la misma, vale decir, hipótesis alternativa que estuvo vigente hasta 31 de agosto de 2024.

Sin embargo, las modificaciones introducidas por la Ley de Delitos Económicos a la Ley 20.393 entraron en vigencia el 1 de septiembre 2024, circunstancia que tuvo el propósito de otorgar a las empresas un periodo de preparación para la entrada en vigencia de la nueva normativa y los importantes cambios que esta traía aparejados. Así, tras la modificación de la Ley 21.595, los presupuestos para que una persona jurídica tenga responsabilidad penal por la comisión de uno de los delitos de la LDI son los siguientes:

a. Se haya cometido un delito informático –sea o no considerado como delito económico, vale decir, sin importar el contexto corporativo– por o con la intervención de alguna persona natural que ocupe un cargo, función o posición en ella, o le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación. También será responsable la persona jurídica por el hecho perpetrado por o con la intervención de una persona natural relacionada con una persona jurídica distinta (ocupando un cargo, función o posición en ella, o prestándole servicios gestionando asuntos suyos ante terceros), siempre que esta le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, o carezca de autonomía operativa a su respecto, cuando entre ellas existan relaciones de propiedad o participación.
b. La perpetración del hecho se ha visto favorecida o facilitada por la *falta de implementación efectiva* de un modelo adecuado de prevención de tales delitos por parte de la persona jurídica.

Por tanto, las exigencias que presenta la nueva normativa son notablemente superiores que las existentes en la actualidad, lo que plantea desafíos importantes para las empresas, que deberán adaptarse a estos estándares superiores. Por ejemplo, se amplía de forma exponencial el ámbito de personas capaces de activar la responsabilidad penal de la

empresa con su conducta delictiva, y se elimina la exigencia de que el hecho ilícito reporte algún provecho o deba haber sido cometido en interés de la persona jurídica. Tampoco basta que se haya implementado un modelo de prevención de delitos, sino que se requiere que dicha implementación haya sido efectiva, real.

Ha destacado en este ámbito el hecho de que la nueva ley aluda directamente al marco de la actividad de la empresa y que, cuando se refiere a la efectividad del modelo de prevención de delitos, manifieste que esa apreciación deberá incluir aspectos como el giro, el objeto social y las actividades de la empresa, entre otros. Ello permite incorporar un aspecto positivo para las organizaciones, en orden a que la evaluación de la efectividad del modelo debe considerar sus propios riesgos; se trata de atender a esa persona jurídica concreta y no a una abstracta. Sin embargo, cuando hablamos de delitos informáticos, nos encontramos ante una cuestión transversal que deja muy poco espacio para que alguna organización pueda omitir considerarlos dentro de sus modelos de prevención.

6. Los delitos informáticos como base del delito de lavado de activos

Finalmente, el artículo 19 de la LDI modifica la Ley 19.913 para incorporar, dentro de los ilícitos que son base del lavado de activos, todos los tipos penales introducidos por esta legislación, desde el ataque a un sistema informático hasta el abuso de los dispositivos.

Esto es relevante porque, en primer lugar, eleva la importancia de la categoría delictiva, incluyendo a los ilícitos informáticos de esta ley en categorías de alta complejidad en lo que a investigación se refiere, y permitiendo, a la vez, un tratamiento más sistemático de las conductas punibles en el marco de la criminalidad organizada. En segundo lugar, tiene la relevancia práctica de permitir la aplicación de todo el estatuto de la Ley de Lavado de Activos, con sus disposiciones específicas y técnicas especiales de investigación, sin perjuicio de lo que se señalará en la parte procesal de este material.

Capítulo 3

Aspectos procesales en matera de ciberdelincuencia y pruebas electrónicas

1. Cuestiones preliminares

Si bien la nueva legislación en materia de ciberdelincuencia, contenida principalmente en la Ley 21.459, ha dedicado un título completo a tratar los aspectos procesales de la materia, este resulta ser bastante menor que el dedicado a las cuestiones penales sustantivas, lo que llama la atención no solo porque este es uno de los aspectos centrales del Convenio sobre Ciberdelincuencia y uno de los objetivos centrales de dicha ley era adaptar nuestro ordenamiento jurídico a este, sino también porque es en este ámbito precisamente donde pueden surgir dificultades en la práctica diaria de los operadores del sistema de justicia criminal, y se pueden presentar los mayores desafíos para, en primer lugar, el órgano de persecución penal y sus auxiliares en la investigación, al pretender obtener la evidencia necesaria para acreditar su teoría del caso, y, en segundo lugar, para el propio órgano jurisdiccional al momento de evaluar el peso de estas probanzas a efectos de emitir su pronunciamiento de absolución o condena, una vez que ha definido que tales antecedentes son admisibles al interior de un proceso penal.

Como se anticipó, solo tres artículos, correspondientes a los números 11, 12 y 14 de la ley, se refieren a los aspectos de índole procesal abordados, esto es, *legitimación activa, técnicas especiales de investigación y preservación, y procedimiento de custodia*. Este último efectúa una remisión a normativa de naturaleza reglamentaria en forma de instrucciones generales emanadas del fiscal nacional del Ministerio Público.

Aunque el artículo 13 también está incluido dentro del Título II de la ley, denominado «Del Procedimiento», en su contenido la norma se refiere al comiso, sin efectuar mayores distinciones que las reglas propias del derecho penal para estos efectos en lo que atañe al inciso primero, en tanto que en su inciso segundo alude al llamado «Comiso por valor

equivalente», institución que ya no es nueva en nuestro sistema,[151] pero que parece explicarse mayormente en esta materia por la característica de inmaterialidad que suelen poseer los efectos e instrumentos de lo que podemos reconocer como ciberdelitos.

Sin embargo, vista desde otra perspectiva, la cuestión no debería extrañarnos desde que hace ya varios años transitamos desde un proceso penal de corte inquisitivo a uno acusatorio, que se caracteriza, entre varios otros aspectos, por la libertad probatoria, la cual rige dentro del *iter* probatorio no solo al momento y durante el proceso de valoración de la prueba, sino también durante la fase de producción misma de ella. En efecto, en serios problemas nos encontraríamos si mantuviéramos un sistema de prueba tasada, en el que los medios de prueba admisibles para la acreditación de los hechos controvertidos estuvieran taxativamente establecidos en la ley, lo que implicaría una indescriptible desconexión del mundo intraprocesal respecto de uno extraprocesal vertiginosamente cambiante en lo que al uso de las tecnologías se refiere.

Afortunadamente, la ley prevé que todos los hechos y circunstancias pertinentes para la adecuada solución del caso sometido a enjuiciamiento podrán ser probados por cualquier medio producido e incorporado en conformidad a la ley, de forma que en la actualidad solo se apunta a la aptitud que tiene el medio de prueba para lograr la convicción del juzgador. Pero sabemos que, previo a que ello ocurra, se exige haber sorteado etapas previas en la incorporación del material probatorio, normas y principios que pueden llevar a que el mismo material resulte excluido, pues aquí cobra relevancia esa permanente tensión entre la eficacia de la persecución penal y los derechos de las personas al interior de un Estado democrático de derecho.

Por las razones previamente expuestas, el contenido de este capítulo excederá la normativa expresa contenida en la Ley 21.459, para abordar otros aspectos que puedan ser de utilidad al momento de enfrentarse, en la práctica, a los desafíos que presentan este tipo de casos. Ello sin perjuicio de ser conscientes que, si en alguna materia emerge de forma importante un riesgo de desfase temporal es en esta, en la que la evolución tecnológica será siempre superior a la capacidad normativa, por lo que los principios jurídicos esenciales y la capacidad de análisis deberían ser los elementos predominantes.

151 La institución también está contemplada, en la actualidad, en la Ley 21.477 y en la Ley 21.595, sobre delitos económicos.

Establecido lo anterior, a continuación se abordarán los aspectos procesales de la normativa sobre ciberdelincuencia con adiciones, pero siguiendo, en lo posible, el orden del texto legal.

2. Inicio del procedimiento. Legitimación activa

Como se ha anticipado, la ley chilena sobre ciberdelincuencia, siguiendo el espíritu del Convenio de Budapest, tiene una significativa pretensión de amplitud, abordando no solo las cuestiones penales asociadas a la cibercriminalidad, sino aquellas de carácter procesal, además de ampliar el rango de responsabilidad penal que afecta a las personas jurídicas, a través de la modificación a la Ley 20.393, y los delitos base de lavado de activos, reformando la Ley 19.913.

De este modo, se transforma en una institucionalidad importante dentro del derecho penal, pero no debe obviarse el hecho de que se trata de una ley penal, de modo que será supletoriamente aplicable a las conductas descritas en la normativa todo el estatuto penal nacional, compuesto, entre otros cuerpos legales, por el Código Penal; el Código Procesal Penal; la Ley 18.216, que establece penas sustitutivas a las penas privativas o restrictivas de libertad; la Ley 21.595, sobre Delitos Económicos, etc.

Así las cosas, y conforme nuestro ordenamiento procesal, la investigación de un hecho que revista las características de un delito informático podrá iniciarse por denuncia, querella de la persona afectada, o bien de oficio por parte del ente persecutor.[152]

La particularidad en este caso, y de acuerdo con lo que dispone el artículo 11 de la ley, está en la posibilidad de que se querellen ciertas autoridades administrativas que no estarían actualmente facultadas para dicho ejercicio sin la existencia de esta norma, pero de forma coherente con lo que existe en otras materias delictivas, en que la intervención de la autoridad para restituir la paz social parece del todo exigible, atendidas las consecuencias de la comisión de dichos ilícitos para los intereses sociales de la comunidad.[153]

---

152 Para los profesores Horvitz y López existe una cuarta modalidad, consistente en la detención en situación de flagrancia. Horvitz y López (2003), pp. 483 y 484. Para nosotras, se trata de una modalidad de denuncia por parte de funcionarios policiales.

153 Ocurre en Ley 18.314, de 17 de mayo de 1984, sobre conductas terroristas (artículo 10), o en el DFL 7.912, de 5 de diciembre de 1927, en lo relativo a los delitos contra el orden y la seguridad públicos.

En efecto, la introducción del actual sistema procesal eliminó también la acción popular consagrada en el artículo 15 del Código de Procedimiento Penal, conforme al cual cualquier persona capaz de parecer en juicio podía ejercer la acción penal por delitos perseguibles de oficio, con la única condición de que dicha posibilidad no le estuviera expresamente prohibida en la ley.[154] En la actualidad, la acción penal corresponde al Estado, a través del Ministerio Público, y fuera de ello queda, en términos generales, acotada a la víctima del delito. Excepcional resulta la posibilidad de una acotada acción popular para las personas que tengan un domicilio dentro de una determinada provincia sean capaces de parecer en juicio y únicamente rige respecto de hechos punibles cometidos en la misma que constituyeren delitos terroristas, o delitos cometidos por un funcionario público que afectaren derechos de las personas garantizados por la Constitución o contra la probidad pública.

Luego, la ley procesal penal deja abierta a otras leyes orgánicas la posibilidad de que órganos y personas puedan querellarse sin revestir la calidad de víctimas directas de un ilícito.

La Ley de Delitos Informáticos, sin ser una ley orgánica de un servicio público, contempla la posibilidad de querellarse para las autoridades y en los casos que señala, de la forma siguiente:

> Artículo 11. Sin perjuicio de las reglas contenidas en el Código Procesal Penal, las investigaciones a que dieren lugar los delitos previstos en esta ley también podrán iniciarse por querella del ministro del Interior y Seguridad Pública, de los delegados presidenciales regionales y de los delegados presidenciales provinciales, cuando las conductas señaladas en esta ley interrumpieren el normal funcionamiento de un servicio de utilidad pública.

De este modo, podemos extraer los siguientes elementos de la norma transcrita:

- Delitos respectos los cuales procede: todos los delitos informáticos que contempla la Ley 21.459, lo que, cabe destacar, no corresponde a todos los ciberdelitos conforme a la conceptualización que hemos venido ofreciendo en este trabajo.

154 Artículo 15: «La acción penal pública puede ser ejercida por toda persona capaz de parecer en juicio, siempre que no tenga especial prohibición de la ley y que se trate de delitos que deban ser perseguidos de oficio».

- Autoridades legitimadas para querellarse: el ministro o ministra del Interior y la Seguridad Pública, el delegado o delegada regional y el delegado o delegada provincial, vale decir, aquellas autoridades administrativas que, en el orden nacional, regional o provincial, tienen entre sus funciones la de velar por que en el territorio de su jurisdicción se respeten la tranquilidad y el orden público, y se resguarde a las personas y sus bienes, para lo cual podrán requerir el auxilio de la fuerza pública, en conformidad a la ley, con lo cual la referencia a ellos y ellas resulta del todo lógica.
- Condición de procedencia: cuando las conductas señaladas en esta ley interrumpieren el normal funcionamiento de un servicio de utilidad pública. Así, la legitimación activa ampliada no solo no rige para todo el campo de los ciberdelitos, sino que, en aquellos para los que está permitida, considera una especial condición de procedencia que apunta al *efecto del delito y su impacto para la población*.

Considerando que tanto las autoridades a las que hace referencia la normativa como los tipos penales contemplados por la misma están claramente delimitados, la mayor posibilidad interpretativa se plantea a propósito del último elemento que la norma contempla, esto es, la necesidad de que las conductas tipificadas interrumpan el normal funcionamiento de un servicio de utilidad pública.

Si bien no existe un concepto único de «servicio de utilidad pública», existen referencias que nos conducen a ciertas materias propias del derecho regulatorio sin que tengan, en cambio, una alusión al carácter público del prestador del servicio. En efecto, el término apunta a actividades, bienes o servicios que buscan obtener un beneficio de carácter colectivo o alcanzar intereses colectivos de un grupo de personas que puede ser muy amplio o más acotado, es decir, no necesariamente debe tratarse de todo el país, sino que podría ser una región o una localidad determinada. Tampoco implica que el servicio deba prestarse de manera gratuita, de modo que, en este contexto, quedan perfectamente incluidas empresas privadas que prestan servicios en utilidad de la comunidad, como electricidad, gas, agua, telecomunicaciones, entre otros. Y la vinculación que existe, en este aspecto, con el mundo privado, de las empresas proveedoras de servicios es una característica que vemos en este y en varios otros aspectos de esta normativa.

Por ello, como correctamente advierten Vera y Mayer, corresponderá a la autoridad que accione en función de la norma en análisis acreditar

que cuenta con la legitimación activa para hacerlo por encontrarse dentro de la hipótesis cubierta por la norma.[155]

En cuanto a que la conducta busque o produzca al menos el efecto de «interrumpir» un servicio de utilidad pública que se establece como la condición habilitante de la facultad de querellarse, atendemos a su acepción regular que, según la RAE, consiste en «Cortar la continuidad de algo en el lugar o en el tiempo», sin que exista ningún marco temporal exigido como mínimo. Así, no es necesario que el servicio permanezca interrumpido para poder querellarse, o algún lapso de tiempo especial de interrupción para encontrarnos ante la hipótesis que la norma contempla.

La otra particularidad que podemos encontrar en la redacción de la norma alude a la referencia de que la querella de las autoridades aludidas, según el texto expreso de la disposición, puede ejercerse para iniciar la investigación. Luego, la pregunta que surge es si, *a contrario sensu*, la facultad no podría ejercerse respecto de investigaciones que ya estuvieren iniciadas, sea por denuncia, de oficio por el Ministerio Público o mediante la interposición de una querella por parte del legitimado original para estos efectos, vale decir, el ofendido por el delito.

Una primera e inmediata respuesta para esta cuestión, ceñida estrictamente al texto de la ley, nos permitiría concluir que la querella solo puede interponerse para iniciar la investigación y no aplicaría respecto de investigaciones en curso, dado que estamos en el ámbito del derecho público –a mayor abundamiento, del derecho penal– y, finalmente, ante una norma excepcional frente a la regla de limitación de la acción popular que nuestro actual sistema contempla.

Sin embargo, creemos que esta no es una lectura correcta y, más bien, lo que la norma quiso hacer, como la primera disposición relativa al procedimiento dentro de la legislación contra la ciberdelincuencia, fue aludir a las formas de inicio de una investigación penal, siguiendo una estricta línea de tiempo. De esta forma, y respetando en lo supletorio toda la regulación procesal penal común, el artículo 11 pretende aportar que, además de aquellas formas de inicio, se suma en esta materia la querella interpuesta por las citadas autoridades ejecutivas, aunque no correspondan a los directamente afectados por el delito. Esa es la particularidad, la admisión de su intervención, y no existe ninguna razón

155 Vera y Mayer (2022b), pp. 319 y 320.

–más que un error legislativo– para limitar esa intervención únicamente a los procedimientos no iniciados. En efecto, si la finalidad en la introducción de esta disposición hubiera sido ampliar el campo de posibilidades de que la *notitia criminis* llegara al ente persecutor, ella hubiera sido totalmente innecesaria desde que para ello bastaba la posibilidad de que las autoridades administrativas en cuestión denunciaran el ilícito, situación presente sin necesidad de ninguna referencia al respecto. Lo que el legislador quiso, entonces, fue dotar de mayor fuerza acusadora a las investigaciones de delitos informáticos cuando la conducta delictiva interrumpiere el normal funcionamiento de un servicio de utilidad pública. De eso se trata, por lo que resulta contrario a la lógica que excluyamos la intervención de las autoridades cuando se trate de procedimientos iniciados. Insistimos: si el objeto hubiera sido solo ampliar las hipótesis de inicio de una investigación, sería probablemente este uno de los casos en que esa necesidad estaría menos presente, dado que, al afectarse un «servicio de utilidad pública», la cantidad de víctimas directas legitimadas para accionar por sí mismas lo haría redundante.

Por tanto, en nuestra opinión, en el caso excepcional de que un tipo penal de los contemplados en la Ley 21.459 interrumpa un servicio de utilidad pública, podrán interponer la respectiva querella criminal las autoridades enunciadas conforme a las normas del CPP –dado que la LDI no ahonda mayormente–, lo que significa que podrán para hacerlo para iniciar una investigación penal y, respecto de investigaciones penales ya iniciadas, dicha facultad se extenderá hasta el cierre de la respectiva investigación, conforme al artículo 112 del CPP, tras lo cual su presentación será extemporánea. En definitiva, se trata de establecer un nuevo sujeto legitimado para *ser* querellante y no únicamente para iniciar un procedimiento por querella, pues para ello bastaba la denuncia y, por ende, no era necesaria la introducción de una norma especial.

A la misma conclusión arriban los profesores Vera y Mayer por distintas razones y sostienen que «[…] teniendo en cuenta que la intervención de dichos sujetos apunta a la salvaguarda del normal funcionamiento de servicios de utilidad pública, según veremos a continuación, resulta conveniente favorecer una interpretación amplia de la norma, que posibilite la intervención de esos organismos, como querellantes, independientemente [de] si con el escrito respectivo se da inicio o no al proceso».[156]

156 Vera y Mayer (2022b), p. 319.

3. Investigación de los delitos informáticos y aspectos probatorios

En esta sección se consideran en detalle las cuestiones previas a la investigación y las características peculiares de la prueba electrónica.

3.1. Cuestiones previas

En materia de ciberdelincuencia, y considerando el principal cuerpo normativo que la regula, el Convenio de Budapest, cabe hacer presente una cuestión esencial: esta normativa no solo aplica para los llamados ciberdelitos, en cualquiera de las categorías que pretendamos agruparlos, o, dicho de otro modo, en el caso de Chile a los tipos penales previstos en la LDI más las figuras de *phishing, pharming* y tipos asociados a la pornografía infantil, entre otros, sino a cualquier conducta delictiva que pueda cometerse por medios informáticos, lo que, sin duda, es materia de ampliación diaria en el mundo digital en el que vivimos. Pero también debe considerarse que esta normativa resulta aplicable a cualquier delito, aunque no sea cometido por la vía tecnológica, en la medida que los medios de prueba que permitan acreditar la conducta tengan soporte electrónico o informático.

Lo anterior constituye un marco de aplicación enorme para el Convenio, dado que los aspectos procesales no quedan limitados a la comisión de los delitos informáticos, sino que, sin temor a equivocarnos, alcanza a cualquier delito que pueda cometerse, pues respecto de cualquiera podríamos encontrar evidencia digital que permita o contribuya al esclarecimiento de los hechos, y pueda ser incorporada como medio de prueba formal al interior de un proceso.

Concretamente, la Sección II del Capítulo II del Convenio instituye las medidas procesales que deben ser adoptadas por los Estados parte, respecto de las siguientes figuras:

1. Los *delitos que el mismo convenio tipifica* y que deben ser adoptados en las normativas nacionales.
2. Cualquier otro *delito cometido por medio de un sistema informático*.
3. La obtención de pruebas electrónicas en la investigación de *cualquier delito*.

Ahora, el Convenio se preocupa de establecer que todos estos procedimientos deben adoptarse para facilitar las investigaciones y procesos penales, pero siempre velando por la protección de los derechos humanos y las libertades personales, lo que expresa la permanente dicotomía del proceso penal que cobra relevancia en un ámbito tan frágil como el del ciberespacio.

No obstante que, para Chile, el Convenio sobre Ciberdelincuencia del Consejo de Europa constituye una ley de la República, que contiene un mandato en orden a establecer las medidas procesales necesarias para la correcta investigación de los delitos informáticos y, superior a ello, para velar por la protección de todas las personas en el ciberespacio, y pese también a que la Ley 21.459 «Establece normas sobre delitos informáticos, deroga la Ley 19.223 y modifica otros cuerpos legales *con el objeto de adecuarlos al Convenio de Budapest*» (énfasis añadido), lo cierto es que no encontramos un desarrollo de dichas medidas en la legislación interna nacional, lo que, en todo caso, no constituye una particularidad de nuestro país, sino que es una situación que se repite en diversos países miembros del Convenio.[157]

Ahora bien, la ausencia de una regulación específica no implica la inaplicabilidad o imposibilidad de incorporación de pruebas electrónicas al interior de los procesos, cuestión que no resistiría análisis en la sociedad actual, primero, por la posibilidad de acudir directamente a la regulación que nos aporta Budapest y, segundo, porque la solución que han generado la mayoría de los ordenamientos como el nuestro se basa en uno de los principios que rige primordialmente la materia probatoria en la actualidad, constituido precisamente por la libertad de prueba. Así, nuestro ordenamiento procesal penal, en el artículo 295 del CPP, permite que todos los hechos y circunstancias pertinentes para la adecuada solución del caso sometido a enjuiciamiento puedan ser probados por cualquier medio producido e incorporado en conformidad a la ley.

157 Así, un trabajo reciente desarrollado por el Programa de Asistencia contra el Crimen Organizado Transnacional de la Unión Europea (El PAcCTO), denominado *La prueba electrónica en el marco nacional y en el internacional en Latinoamérica* (2022), concluye que «(…) cuantitativamente son pocos los países miembros de El PAcCTO que cuentan con legislación específica en materia de normas procesales penales que prevean de manera especial medios de prueba adaptados a las necesidades que plantea la prueba digital». Luque *et al.* (2022), P. 22.

La norma en cuestión, y, previo a ella, el principio que la misma alberga, le otorga la necesaria flexibilidad a la legislación, la protege ante el riesgo de obsolescencia y asigna un rol importante a los operadores del sistema, principalmente a los jueces, de establecer los estándares que deban primar en materia probatoria, comenzando, por supuesto, por la obtención misma de la evidencia, la que deberá cumplir con ciertas cualidades tradicionales que se fundan en el respeto de los derechos fundamentales de las personas.

Sin perjuicio de comprender la situación anterior y la necesaria plasticidad que las normas deben tener en una materia altamente evolutiva como la relacionada con la tecnología, no puede desconocerse que, por una parte, el carácter fuertemente especializado de estos aspectos probatorios y, por otra, la vulnerabilidad e importancia de los derechos potencialmente afectados, recomendarían contar con una regulación que aspirara a constituirse en una verdadera guía de apoyo para los operadores de la ley, especialmente para la judicatura, y que al mismo tiempo contribuyera en materia de certeza jurídica.

En efecto, la certeza jurídica es una garantía básica que los Estados deben contemplar para sus justiciables. Implica, por cierto, el principio de legalidad (*nullum crimen nulla poena sine lege*), pero no solo apunta a que la ley exista, sino también a que cumpla con ciertos aspectos de calidad, que sea accesible, clara y previsible. Se apunta a la accesibilidad de la información en cuanto a la posibilidad de conocer las consecuencias de la conducta de cada persona. El Tribunal Europeo de Derechos Humanos ha tenido la posibilidad de pronunciarse sobre este punto en el caso de *Roman Zakharov v. Russia*, que se refería a la interceptación general de las comunicaciones mediante reglamentos internos, dado que en Rusia las empresas de telefonía móvil estaban obligadas a instalar equipos que permitieran a las fuerzas de orden realizar actividades de registro que, sin regulación, se convertían en interceptaciones de carácter general, razón por la que el jefe de una editorial decidió recurrir ante la Corte superior, que señaló categóricamente que la ley debía cumplir requisitos de calidad: debe ser accesible para la persona interesada y previsible en cuanto a sus efectos.[158] En el mismo sentido se pronuncia

158 *Roman Zakharov v. Russia*, TEDH 47143/06, en su párrafo 228 dispone: «The Court notes from its well-established case-law that the wording 'in accordance with the law' requires the impugned measure both to have some basis in domestic law

la sentencia en el caso *Liviik v. Estonia*: «[…] El término 'ley' implica requisitos cualitativos, incluidos los de accesibilidad y previsibilidad. Un individuo debe saber por la redacción de la disposición pertinente y, si fuera necesario, con la asistencia de los tribunales, su interpretación de la misma, qué actos y omisiones le harán penalmente responsable y qué pena se impondrá por el acto cometido y/u omisión. Además, una ley aún puede satisfacer el requisito de 'previsibilidad' cuando el interesado debe recurrir al asesoramiento jurídico adecuado para evaluar, en un grado que sea razonable dadas las circunstancias, las consecuencias que una determinada acción puede implicar».[159]

Con la finalidad de contribuir al desarrollo en esta materia, en este trabajo abordaremos aspectos generales de la prueba electrónica, para luego aludir al tratamiento específico de ella en el Convenio de Budapest y terminar con las normas específicas que contiene nuestro ordenamiento interno, tanto en la LDI como en otros cuerpos legales. Insistimos que solo se trata de aspectos generales, pues una exposición íntegra y un detallado análisis de la prueba digital exigirían un tratado específico.

Finalmente, hacemos presente que este desarrollo utilizará en importante medida doctrina, legislación y jurisprudencia españolas, por tratarse de un país que cuenta con una cultura e idiosincrasia similar a la nuestra, pero con mucho mayor avance en este punto, puesto que España adhirió al Convenio sobre Ciberdelincuencia del Consejo de Europa en el año 2010, con lo cual en el año 2015 adecuó su normativa procesal penal a dicho instrumento internacional mediante la modificación a su Ley de Enjuiciamiento Criminal por la Ley Orgánica 13/2015, para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, de 6 de diciembre de 2015.

3.2. Generalidades en materia de prueba electrónica

Se pasa a revisar de manera particular cada aspecto relevante en materia de prueba electrónica.

---

and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. *The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects* […]» (*én*fasis añadido).

159 *Liviik v. Estonia*, TEDH 12157/05, párrafo 93.

A) Concepto y naturaleza jurídica de la prueba electrónica

Lo primero que cabe comentar en este punto es que no existe una definición legal de la prueba electrónica, sin perjuicio de que hay varias aproximaciones doctrinarias. Por lo mismo, nos parece que cualquier análisis debe comenzar por la ciencia procesal en general y, en este sentido, cobra utilidad la clásica distinción del tratadista italiano Carnelutti entre fuentes de prueba y medios de prueba. Así, las fuentes de prueba son conceptos preexistentes al proceso (la parte, el testigo, el documento, la cosa que ha de ser examinada, el conocimiento técnico del perito) y los medios de prueba son conceptos que existen en y para el proceso (interrogatorio de las partes o de testigos, reconocimiento judicial, dictamen de peritos, etc.).[160] En nuestro sistema de justicia criminal, el órgano persecutor, esto es, el Ministerio Público con el apoyo de sus auxiliares en la investigación –que probablemente cobren mucha mayor relevancia en este ámbito en virtud de la pericia técnica requerida–, deberá indagar respecto de la existencia de ilimitadas fuentes de prueba que puedan existir para el esclarecimiento de los hechos constitutivos de delito, las que, en el momento en que se pretenda incorporarlas como evidencia, deberán cumplir con las exigencias propias que apuntan a la licitud en su obtención, cuestión supervisada en sede judicial, todo lo que, posteriormente y en la medida que sea útil para acreditar la teoría del caso, deberá incorporarse formalmente en el proceso como un medio de prueba que constituirá uno de los elementos para que el órgano jurisdiccional forme su convicción en un sentido u otro.

En tal sentido, como fuente de prueba el persecutor debe considerar siempre la posibilidad de que cualquier dispositivo o equipo electrónico que sea encontrado en el marco de una investigación pueda aportar medios de prueba que posteriormente sean útiles al esclarecimiento de los hechos, y ello es importante porque muchas veces su utilidad puede no ser evidente ni estar a la vista del investigador, lo que exige la formación de capacidades especiales en este ámbito. Sin embargo, lo anterior no implica en caso alguno –como se detallará más adelante– que estén permitidas operaciones generales o «expediciones de pesca» por parte de la policía y el persecutor, por cuanto estas resultan atentatorias contra los derechos fundamentales de las personas afectadas por dichas medidas.

160 Carnelutti (2000), pp. 37 y ss.

Como fuentes de prueba, entonces, podemos reconocer computadores, teléfonos móviles, *tablets*, cámaras digitales, videocámaras digitales, grabadores de audio, consolas de videojuegos, impresoras, escáneres, circuitos cerrados de televisión, televisores «smart», *quick response codes* (códigos QR), localizadores GPS, tarjetas de memoria, discos compactos, reproductores multimedia portátiles, entre muchos otros que existen actualmente y que van aumentando diariamente. Pensemos que incluso un iris, mediante su reconocimiento, o una huella dactilar, en cuanto clave biométrica, podrían constituir prueba electrónica en la medida que permitan validar procesos u operaciones en un determinado sistema informático.

En cuanto a la actividad probatoria, sabemos que existen múltiples definiciones a su respecto y que pasan también por entender que, dentro de esta actividad puede haber una diligencia de averiguación como una de comprobación, pero que, en lo importante, implica introducir ciertos elementos al interior del proceso, que permitan al juzgador adquirir convicción respecto de la forma en que han acaecido los hechos materia de su pronunciamiento. Así, siguiendo a Taruffo, se trata del instrumento que utilizan las partes desde hace siglos para demostrar la verdad de sus afirmaciones, y del cual se sirve el juez para decidir acerca de la verdad o falsedad de los enunciados fácticos.[161] Se suele situar como punto central en materia probatoria su capacidad para formar la convicción del juez y, si esto es así, es perfectamente posible incorporar los medios digitales como parte del abanico de instrumentos que pueden servir a las partes para demostrar la veracidad de sus afirmaciones y lograr la convicción del juzgador.

En definitiva, la prueba electrónica puede incluirse en la mayor parte de las definiciones doctrinarias de prueba. Si bien existen diferencias importantes atendiendo al régimen probatorio del que se trate, en especial si nos encontramos ante un sistema de prueba libre o uno de prueba legal o tasada, en cualquier caso, estará presente el elemento relativo a su aptitud para generar convicción judicial. Sin duda la existencia de sistemas de prueba tasada haría que la incorporación de nuevos medios probatorios se tornara dificultosa en ausencia de disposición legal, y exigiría una actualización legislativa difícil de acompasar con los avances tecnológicos, lo cual es una razón más para privilegiar los sistemas de prueba libre sobre los legales.

161 Taruffo (2008), p. 59.

Según la Guía de Prueba Electrónica del Consejo de Europa,[162] la prueba electrónica es aquella información o datos que han sido creados, almacenados o transmitidos a través de dispositivos electrónicos y tienen relevancia en un procedimiento judicial.

Conforme a Delgado Martín,[163] por prueba electrónica cabe entender toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio. En esta definición cabe destacar los siguientes elementos: se refiere a cualquier clase de información; esta ha de ser producida, almacenada o transmitida por medios electrónicos; y ha de ser capaz de tener efectos para acreditar hechos en el proceso abierto para la investigación de todo tipo de infracciones penales, y no solamente para los denominados delitos informáticos.

De esta manera, la fuente de la prueba radica en la información contenida o transmitida por medios electrónicos, mientras que el medio de prueba será la forma a través de la cual esa información entra en el proceso: normalmente como prueba documental o como prueba pericial, pero también incluso a través de la prueba testifical, mediante el testimonio de la persona que ha tenido contacto con el dispositivo electrónico.[164]

El mismo autor advierte que dicho concepto permite englobar dos tipos de prueba electrónica: aquella que se refiere a información *almacenada* en un dispositivo electrónico y la que denota información *transmitida* por redes de comunicación abiertas o restringidas. Pero, en cualquiera de estos casos, corresponde a antecedentes que deberán recopilarse conforme a los principios que rigen la actividad probatoria e incorporarse de la misma forma al eventual juicio que se desarrolle.

El autor español Bueno de Mata[165] configura un concepto unánimemente aceptado de prueba electrónica, definiéndolo como «cualquier

162 La Guía sobre Prueba Electrónica es la herramienta de apoyo más importante del Consejo de Europa en relación con las pruebas electrónicas. Fue elaborada en 2013 en el marco del proyecto conjunto del Consejo de Europa y la Unión Europea CyberCrime@IPA. Su contenido fue coordinado por Nigel Jones (Reino Unido). Expertos en ciberseguridad de los países integrantes del CyberCrime@IPA y expertos de otros países (África, Asia y Europa) y otras áreas de conocimiento contribuyeron también a su desarrollo. No es un documento público, pero puede solicitarse a través de la Comunidad Octopus de la lucha contra la ciberdelincuencia del Consejo de Europa: https://www.coe.int./en/web/octopus/request-form.

163 Delgado (2013), *passim*.

164 *Ídem*.

165 Federico Bueno de Mata, citado en Sánchez (2016), p. 8.

información obtenida a partir de un dispositivo electrónico o medio digital que sirva para adquirir convencimiento de la certeza de un hecho, siempre que sea correctamente obtenida, constituyendo así pruebas exactas, veraces y objetivas». Después puntualiza que se entiende por prueba electrónica «aquel medio electrónico que permite acreditar hechos relevantes para el proceso, ya sean físicos o incluso electrónicos, y que se compone de dos elementos necesarios para su existencia, los cuales delimitan la especialidad de la prueba electrónica en relación al resto de medios probatorios: un elemento técnico o *hardware*, y un elemento lógico o *software*».[166]

Respecto de la naturaleza jurídica de la prueba electrónica, básicamente existen tres posiciones:[167]

- Tesis analógica: cronológicamente, es la primera en surgir y tiende a hacer equivalente la prueba electrónica y la prueba documental, con base en las similitudes entre ambas. De esta forma, la aplicación de este tipo de prueba debería ceñirse a las normas procedimentales previstas para la prueba documental.
- Tesis autónoma: considera que la prueba electrónica es independiente de la documental y, si se pretende hacer valer en un proceso, se necesita no solo de la licitud en su obtención, sino de la posterior verificación o autenticación de la autoría y de las afirmaciones formuladas. De acuerdo con los autores partidarios de esta tesis, la modalidad se envuelve dentro de los instrumentos de filmación, grabación y semejantes, esto es, de los instrumentos que permiten archivar, conocer o reproducir datos relevantes para el proceso.
- Tesis de la equivalencia funcional: finalmente, esta tesis entiende que el contenido de un documento electrónico surte los mismos efectos que el contenido de un documento en papel. En otras palabras, la equivalencia funcional implica aplicar a los mensajes de datos un principio de no discriminación respecto a las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas; en este sentido, los efectos jurídicos deseados por el emisor de la declaración deben producirse con independencia del soporte en papel o electrónico donde conste la declaración.

166 *Ídem*.
167 Sánchez (2016), p. 8-10.

Actualmente, la tesis de la autonomía es la mayoritaria, en tanto la analógica la minoritaria.

B) Características de la prueba electrónica

Más allá de clasificaciones tradicionales, como aquella que distingue entre prueba directa o indirecta, preconstituida o circunstancial, o su peso probatorio en un sistema rígido de valoración de la prueba, este párrafo apunta a la necesidad de detenernos en ciertos rasgos específicos de la prueba electrónica, que justifican el tratamiento que se hará en los apartados siguientes. Entre estas características, podemos mencionar las siguientes[168]:

i. Volatilidad: esta característica es intrínseca de la prueba electrónica y apunta a su fragilidad, a lo fácil que resulta alterarla, dañarla o destruirla en comparación a cualquier otro medio de prueba, lo que, a su vez, implica mayores exigencias en materia de cadena de custodia.
ii. Intangibilidad: la evidencia digital, por su propia naturaleza, no es accesible mediante los sentidos de manera directa, no puede verse ni tocarse. Para conocerla e interpretarla necesitamos tanto de un *hardware* como de un *software* y, dependiendo la complejidad de la evidencia, podemos también necesitar el apoyo de una persona capacitada que nos apoye en ese conocimiento e interpretación. Se dice que se trata de evidencia que puede ser invisible a los ojos de personas inexpertas.
iii. Latencia: esta característica apunta a que la evidencia, a primera vista, no permite percibir qué información es la que contiene en su interior, sino que para ello se debe recurrir a un examen a través de instrumentos y procesos forenses específicos.
iv. Capacidad de duplicación: nos referimos a la posibilidad de copiar la evidencia no una vez sino indefinidamente, sin que ello implique ninguna degradación para el material original.
v. Existencia de metadatos: se trata de un conjunto de datos que describen el contenido informativo de un recurso, de archivos o de información de los mismos. Vale decir, se trata de información que describe otros datos, como el tamaño de un archivo, su fecha de

168 Siguiendo a Regali (2021), s.p., lo que es coincidente en buena medida con las características anotadas en la Guía sobre Prueba Digital del Consejo de Europa.

creación, el historial de modificaciones. Se dice que son «los datos de los datos».

C) Principios que informan el tratamiento de la prueba electrónica

La cuestión apunta a los requisitos que se exigen a la prueba electrónica para que esta pueda ser admitida válidamente al interior de un proceso, especialmente anotadas las peculiaridades referidas en el punto anterior. Se trata, por tanto, de una cuestión aplicable a toda prueba, pero que reviste ciertas particularidades tratándose de probanzas de carácter digital.

En términos de la admisibilidad de la prueba, el juez deberá ponderar ciertos requisitos, algunos intrínsecos y otros extrínsecos, conforme la categorización efectuada por el profesor Devis Echandía; los primeros atañen al medio mismo utilizado en cada caso, incluyendo su objeto, y los segundos se refieren a circunstancias que existen separadas de ese medio, pero que se relacionan con él y lo complementan. Son requisitos intrínsecos: a) la conducencia del medio; b) la pertinencia o relevancia del hecho objeto de la prueba; c) la utilidad del medio; d) la ausencia de prohibición legal de investigar el hecho. Son requisitos extrínsecos: a) la oportunidad procesal o ausencia de preclusión; b) las formalidades procesales; c) la legitimación y postulación para la prueba de quien la pide o la presenta y la legitimación del juez que la decreta; d) la competencia del juez o de su comisionado; e) la capacidad general del juez o funcionario comisionado y de los órganos de la prueba (testigos, peritos, intérpretes, partes cuando confiesan) y la ausencia de impedimentos legales en aquellos y estos.[169]

Lo cierto es que es posible aplicar en esta materia los principios propios de la actividad probatoria en general, pero cuando aludimos específicamente a la prueba electrónica, podemos referir ciertos principios específicos que, si bien también pueden ser aplicables en términos generales, cobran mayor vigor en este ámbito. Entre ellos están los siguientes:

i. Integridad: este principio apunta a que en la manipulación de los dispositivos y datos electrónicos exista especial cuidado en evitar alteración, tanto de *hardware* como de *software*. La evidencia debe mantenerse íntegra desde el comienzo y durante todo el

169 Devis (2002), *passim*.

procedimiento, para lo cual deben seguirse protocolos específicos y el personal involucrado ha de contar con la formación necesaria. Si bien este es un principio que rige para toda actividad probatoria, cobra mayor fuerza tratándose de evidencia de estas características por su condición de especial volatilidad. Por tanto, la cadena de custodia debe ser particularmente pulcra.

ii. Autenticidad: con relación al principio anterior, se trata de que la prueba digital sea capaz de establecer los hechos de forma que no puedan ser discutidos, pues son fiel representación del estado original del material.

iii. Repetitividad y auditabilidad: a este respecto se señala que resulta imprescindible registrar con precisión toda la actividad en el lugar de los hechos, para que un tercero pueda reproducir las acciones ejecutadas desde el primer interviniente de ser necesario. En definitiva, se trata de que todo el procedimiento resista una labor de auditoría y que, al reproducirse todos los pasos, se garantice que se llegaría al mismo resultado.

iv. Exhaustividad: el análisis o cualquier opinión basada en las pruebas debe contener toda la historia y no puede presentarse de manera sesgada.

v. Licitud o legalidad: de nuevo nos encontramos con un principio común a la actividad probatoria, pero lo relevamos por la especial vulnerabilidad que todas y todos podemos padecer en el mundo digital. En efecto, se trata de un espacio en el que se encuentran nuestros datos personales, donde puede conocerse parte importante de nuestra intimidad, donde está en juego nuestra libertad de expresión, etc. En definitiva, la potencial afectación de derechos fundamentales que puede existir en esta materia exige relevar el apego estricto a la ley y al Estado de derecho, y el respeto por los derechos de todas y todos en el ciberespacio. Esto, por un lado, excluye la realización de «expediciones de pesca» y, por otro, exige el cumplimiento de determinados requisitos entre los que estará la obtención de las autorizaciones judiciales cuando sea del caso.

vi. Proporcionalidad: se trata de la aplicación de un principio clásico en el ámbito jurídico en general y, particularmente, cautelar penal. Estamos hablando de medidas intrusivas y vulneratorias de derechos de personas, por lo que la finalidad de esclareci-

miento de los hechos debe justificar esa lesión. Dicho de otro modo, la afectación del derecho no debería ser superior al valor probatorio de la evidencia en cuestión.

vii. Especialización y formación adecuada: apunta al óptimo, que deriva también de las características técnicas de este tipo de prueba, que exige la participación de especialistas en pruebas electrónicas siempre que ello sea posible, es decir, que estén involucradas personas que cuenten con conocimientos adecuados y comprobables en la materia que las habiliten para el tratamiento de la evidencia. En el evento de que ello no sea posible, se debe velar por que los primeros intervinientes que registren o incauten la información, o accedan a ella, sean personas capacitadas para llevar a cabo el procedimiento conforme la normativa jurídicamente aplicable, y que luego puedan ser capaz de explicar sus operaciones ante el persecutor y el órgano jurisdiccional, según se requiera. No significa que todo constituya una pericia, sino que simplemente las operaciones deben hacerse por quien corresponda, así como la extracción misma de una muestra de ADN no es una pericia, pero debe realizarse conforme a ciertos protocolos y por personas capacitadas.

Insistimos en que, con este resumen, hemos querido referir aquellas cuestiones esenciales que deben ser cumplidas con la finalidad de que determinados antecedentes, datos o información de carácter electrónico puedan ser introducidos en el marco de un proceso judicial y que, por las razones en cada caso expuestas, se estima que ameritaban ser relevadas. En caso alguno se pretende excluir la aplicación de los principios formativos en la actividad probatoria en general que, como materia de prueba que es, le resultan plenamente aplicables. Así, por ejemplo, la bilateralidad de la audiencia ocupará siempre un rol primordial al interior de todo proceso en que se incorpore prueba de carácter electrónico.

D) Etapas que envuelve la incorporación de la prueba electrónica en el proceso penal

En general, el *iter* probatorio o procedimiento que contempla cada prueba dentro del ámbito procesal reconoce las etapas de proposición, admisibilidad, ejecución y valoración. En el ámbito penal, en consideración a los bienes jurídicos que están en juego, cobra especial relevancia

la obtención de aquella evidencia que, posteriormente, será introducida formalmente en el proceso. Por ello, y no siendo exclusiva de este ámbito, es en el campo procesal penal en el que se ha desarrollado más profundamente el estudio de la prueba ilícita, de su efecto contaminante, de la prueba derivada, de las exclusiones probatorias y de las excepciones a las reglas de exclusión, en función de atenuaciones de la ilicitud inicial u otras. La prueba electrónica no solo no está exenta de la aplicación de dichos estándares, sino que, incluso, puede decirse que ellos se ven particularmente exigidos en esta esfera.

En materia de obtención de la evidencia electrónica, rige íntegramente la legalidad, juridicidad y proporcionalidad para una medida de intrusión. Cómo obviar la importante afectación al derecho a la intimidad si consideramos que un dispositivo electrónico es una prolongación artificial de nuestra memoria que conserva datos que permiten conocer nuestras amistades, pensamientos y hasta movimientos. Y el peligro reside en que podría hacerse un perfil psicológico concreto de la persona, así como conocerse su situación económica, social y familiar.[170]

En definitiva, a la base de este tipo de diligencias veremos comprometido el derecho a la intimidad, sin perjuicio de considerar otras afectaciones, como al secreto de las comunicaciones, la autodeterminación informativa, la protección de datos personales y, eventualmente, la inviolabilidad del hogar, si ello se produce en el marco de una diligencia de entrada y registro.

La propia multiplicidad de los instrumentos y elementos tecnológicos determina una heterogeneidad de las formas de acceder a su contenido. En efecto, cuando hablamos de obtención de evidencia electrónica podemos encontrarnos en distintos supuestos:

- Obtención de información desde un dispositivo electrónico mediante la aprehensión material del mismo.
- Obtención de información desde un dispositivo electrónico mediante el registro remoto del mismo.[171]

170 Borges (2018), pp. 536-549.

171 Velasco (2011), pp. 22 y 23, destaca diferentes ventajas de la utilización de los «troyanos», tales como que exigen menos efectivos investigadores que cualquier otra técnica tecnovigilante y captan muchísima más información; se instalan con alta movilidad, ya que operan a través de Internet mediante distintas máquinas, técnicas, plataformas y arquitecturas, de modo que son tan ubicuos e instantáneos como la actividad transnacional y transfronteriza que desarrolle el investigado; y

- Obtención de información desde un dispositivo electrónico mediante un agente informático encubierto.[172]

Ahora, respecto del *continente*, pueden distinguirse dos situaciones:[173]

- Acceso a los datos contenidos en el propio sistema informático o equipo de almacenamiento (registro tradicional).
- Acceso a los datos existentes en otro sistema de información accesible desde el primero o disponible para este. Vale decir, un registro remoto que nos lleva al campo de la deslocalización de la información mediante técnicas de computación en la nube.

Cada una de estas actuaciones, en el caso concreto y en las circunstancias específicas, debe ser llevada a cabo con respeto a los derechos fundamentales de las personas, lo que constituye una de las preocupaciones centrales del Convenio de Budapest, conforme lo expone su artículo 15:

Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.
2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguar-

---

aprovechan la tecnología para multiplicar la velocidad de conocimiento de la actividad investigada porque, según la concreta programación del *software* espía, este busca y selecciona lo investigado más rápidamente que el propio agente facultado. Como desventajas, el mismo autor señala que pueden ser detectados por los programas antivirus, a no ser que se solicitase la impensable colaboración de los proveedores de antivirus, y que para su instalación se precisa de una conexión a Internet lo suficientemente consistente como para que dé tiempo a alojar el *software*.

172 Rodríguez (2017/2018), pp. 11-19.

173 Delgado (2013), s.p.

dias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

Cotejando esta disposición con nuestra legislación interna, particularmente los artículos 19 número 4 de la CPR y 9° del CPP, sabemos que la obtención de la evidencia requerirá de la previa autorización judicial por parte del órgano facultado para tales efectos, esto es, el juez de garantía.

En España, el desarrollo doctrinario y jurisprudencial ha llevado a establecer cuatro fases en la obtención de la evidencia: (1) aprehensión o incautación del dispositivo, (2) registro de su contenido, (3) acceso a la información en su interior, y (4) obtención y confiscación de los datos.[174] La autorización judicial se requeriría por separado para cada de las actividades, que afectarían distintas garantías constitucionales.

Pero no basta que la evidencia haya sido obtenida con pleno respeto a los derechos fundamentales de los afectados, sino que estos deben seguir siendo resguardados con posterioridad, particularmente en lo que se refiere al derecho a defensa. Por ello deben considerarse las peculiaridades de la prueba electrónica conforme lo anotamos en forma previa.

Así, sus características de volatilidad y facilidad de manipulación conllevan la exigencia de resguardarla debidamente, velando por su integridad y autenticidad. Estos desafíos deben afrontarse adecuadamente, pues las ventajas de este tipo de evidencia son bastante claras en términos de la claridad y objetividad de la información, de la falta de contradicción de los elementos que podemos encontrar en ellas y de que, en definitiva, redundarían en una justicia más moderna y eficaz. Sin embargo, la posibilidad de adulteración, con las consecuencias que ello puede traer aparejadas sobre todo en el ámbito de la justicia penal, hace que este sea uno de los puntos críticos en la materia.[175]

174 *Ídem*.

175 La utilidad de estos medios de prueba para el esclarecimiento de los hechos resulta innegable. Piénsese, por ejemplo, en que gracias a la existencia de una cámara

Es decir, cuando hablamos de licitud o ilicitud, la cuestión se concreta en la conveniencia inexorable de que las evidencias digitales se hayan obtenido sin violación o merma de los derechos fundamentales reconocidos en la Constitución. El juicio de fiabilidad, por su parte, se refiere a la posibilidad de comprobar la autenticidad e integridad de los documentos digitales obtenidos y el hecho de que no han sido manipulados.[176]

Por ello, y a falta de regulación legal, pero conscientes de la necesidad de avanzar en el establecimiento de estándares que aporten certidumbre y seguridad jurídica para aprovechar el enorme valor probatorio de estos antecedentes, en la doctrina y jurisprudencia española han surgido algunos parámetros que parece importante traer a colación, conjuntamente con ciertas disposiciones y orientaciones de la Guía sobre Prueba Electrónica del Consejo de Europa, a la que hemos aludido previamente. Estos parámetros son los siguientes:

i. Clonado o vaciado de datos.
ii. Presencia de ministro de fe.
iii. Presencia del investigado.
iv. Cadena de custodia.

Respecto de los puntos ii y iii, la jurisprudencia del Tribunal Supremo español ha señalado que no constituyen requisitos de validez para la admisibilidad de la prueba, vale decir, que no anulan su valor. Por el contrario, mucha mayor atención se pone en materia de clonado y, sobre todo, de cadena de custodia.

El proceso necesario para garantizar la fiabilidad y autenticidad de la evidencia, en forma previa a los pasos enunciados, requiere considerar la importancia de la primera operación, que es la extracción, por lo cual, y siguiendo las indicaciones del Consejo de Europa, es importante que el registro se documente de principio a fin. Que en lo relativo a la escena física se elabore un mapa de toda la red y las configuraciones informáticas, se tomen fotografías, se hagan grabaciones de video, etc. Debe dejarse constancia de los dispositivos que están funcionando y los que no. La importancia del personal calificado vuelve a la carga en este punto,

---

de vigilancia podemos contar en forma permanente con un «testigo presencial» de la comisión de hechos delictivos, no afectado por eventuales problemas que pueden aquejar a la memoria humana y que, dependiendo de la resolución del dispositivo, puede incluso acreditar plenamente la participación punible.

176 González (2021), pp. 43-79.

puesto que solo él o ella sabrá distinguir, por ejemplo, entre un escenario *post mortem* y uno en vivo, y las exigencias que la práctica aconseja contemplar para cada caso.[177]

A. CLONADO O VACIADO DE DATOS

Se trata de un procedimiento informático ajeno a la ciencia jurídica pero sumamente importante al momento de garantizar que el material originalmente extraído se ha mantenido inalterable durante el curso de la investigación y al momento de su incorporación como medio de prueba al proceso judicial. En general, el análisis sobre el material recopilado no debería hacerse sobre el soporte original, sino sobre copias. Ya decíamos que una de las características esenciales de la prueba electrónica radica en la posibilidad de duplicarla cuantas veces sea necesario. Esta primera operación consiste en la realización de una copia espejo, bit a bit, de la información digital original. Desde el punto de vista jurídico, el clonado constituye una *garantía de fiabilidad* en el registro y análisis de los dispositivos que permite acreditar la *mismidad*[178] de lo aprehendido, esto es, que lo que se copia es imagen fiel de lo copiado o intervenido.[179]

Mediante este procedimiento deberá generarse un original de los datos, una copia resultado del clonado que será sobre la cual se practicará la pericial informática, y una segunda copia para el titular de los datos, para el caso de que fuese necesario que el mismo continuase con la actividad que viniese ejerciendo. Deberá, por cierto, levantarse un acta de la operación, con los datos de individualización del titular y todos los demás elementos que aseguren el material probatorio, como precintos, embalajes y el señalamiento de quién es en adelante responsable de los dispositivos intervenidos.

177 El escenario *post mortem* se refiere a los equipos apagados que se han encontrado en el registro, los que deben ser retirados del lugar y examinados posteriormente en un laboratorio forense. En cambio, si un dispositivo no está apagado y se encuentra en funcionamiento, se debe considerar la posibilidad de realizar una investigación forense en vivo, a fin de recopilar datos volátiles como el contenido de memoria RAM que puede contener, por ejemplo, claves de cifrado. El hecho de apagar un dispositivo en funcionamiento puede comprometer el acceso a evidencia útil y el posible acceso a dispositivos conectados o a volúmenes cifrados abiertos.

178 El término ha sido reiteradamente utilizado por el Tribunal Supremo español para aludir al carácter íntegramente inalterado de la evidencia.

179 González (2021), pp. 43-79.

Lo que se realiza en la actividad de clonado básicamente es una copia física del contenido del dispositivo. Pero es mediante el *hash*, una función basada en algoritmos que otorga al contenido de un archivo un valor numérico, como se corrobora que los datos que se encontraban en el dispositivo original no han sido manipulados y, por tanto, son los mismos que los que se hallan en la copia.

B. PRESENCIA DE UN MINISTRO DE FE

Se trata de un requisito que contempla la Ley de Enjuiciamiento Criminal española, pero que, sin embargo, conforme a pronunciamientos de la Audiencia Nacional y del Tribunal Supremo de ese país, no constituye un requisito de validez de la actuación[180] y, por tanto, su ausencia no atenta contra la autenticidad del material. En efecto, no solo se trata de un proceso largo en que se exigiría la presencia del letrado, sino que el aporte de este, en la medida que no tiene mayores conocimientos informáticos, nada contribuiría a la diligencia. Su mayor aporte dice relación con hacer fe respecto del número IMEI[181] del dispositivo incautado, número de serie, etc.

C. PRESENCIA DEL IMPUTADO

Se trata también de un requisito contemplado en la Ley de Enjuiciamiento Criminal española, pero que, en el mismo sentido anterior, ha sido declarado como no esencial por la jurisprudencia de los tribunales.[182] Esto no implica desconocer el principio de contradicción que rige también –y, por supuesto, con fuerza– en materia probatoria, pues tal posibilidad estará plenamente vigente en las etapas procesales correspondientes.[183]

---

180 Entre los pronunciamientos, están STS 256/2008 de 14 de mayo y STS 1599/1999 de 15 de noviembre.

181 Por sus siglas en inglés *International Mobile Equipment Identity*.

182 En este sentido, sentencia 34/2014 de 24 de julio de la Audiencia Nacional y STS 187/2015 de 14 de abril.

183 En sentido contrario, Regali (2021), *passim*, quien señala que «La facultad de control, implica para las partes, garantizar la posibilidad de examinar la producción de las evidencias de la contraria y de controvertirla en el caso de considerar que la misma fue obtenida de manera ilegal, a través de un método erróneo, con intervención de personal no capacitado, etc.

En consecuencia, y consonancia con lo desarrollado anteriormente, entiendo que

D. CADENA DE CUSTODIA

A riesgo de ser reiterativas, insistimos en que las especiales características de la prueba electrónica, básicamente en términos de su volatilidad y capacidad de alteración, eliminación, duplicación, etc., hacen que nos encontremos ante un material que presenta retos importantes en materia de conservación. Y esos desafíos no son en absoluto nimios, sino, por el contrario, esenciales, porque resulta imprescindible que lo que en algún momento se intervino, luego fue trasladado y más tarde presentado ante el órgano jurisdiccional para su examen conforme a principios de inmediación, publicidad y contradicción sea exactamente lo mismo («mismidad», en términos del Tribunal Supremo español), pues ello es lo que servirá para que este último determine o no que le cabe responsabilidad penal a una persona por la comisión de un hecho punible, con las consecuencias que ello conlleva.

Si bien no existe una definición legal de este concepto, el propio Tribunal Supremo español, en STS 491/2016 de 8 de junio de 2016, aporta una definición cuando señala que «la cadena de custodia es el proceso transcurrido entre que los agentes de la policía intervienen un efecto del delito que puede servir como prueba de cargo, hasta que se procede a su análisis, exposición o examen en la instrucción o en el juicio».

Propio de cualquier elemento probatorio es su confiabilidad al momento en que el tercero imparcial debe estudiarlo para, conjuntamente con las demás probanzas, obtener su convicción. Si el proceso llamado a otorgarnos esa confianza se ha roto en alguna de sus etapas, es la autenticidad de la prueba la que se ve en riesgo. Ahora, el proceso no es automático ni absoluto. Vale decir, no basta con alegar alguna irregularidad o especular sobre la base de lo que pudo haber pasado, sino que deberá acreditarse que existió esa irregularidad.[184] Por otro lado, una infracción

---

el acto de extracción de la información, u obtención de la evidencia digital (no obstante, su estado latente) debe ser controlado por la contraparte (o al menos asegurar la posibilidad de control), ante el riesgo posible de que dicho procedimiento no pueda reproducirse luego.

Considero que la consecuencia jurídica de no garantizar la presencia de la contraparte en el momento de la obtención de la evidencia digital (con la debida notificación del día, lugar, hora e identidad de quien realizará el procedimiento) deberá ser su nulidad (por violación al debido proceso y a la facultad de control) y por ende su exclusión probatoria».

184 Pero no basta con que la parte que pretende alegar la ruptura de la cadena

de escasa relevancia no determina por sí misma la exclusión de la prueba del proceso, «por lo que la misma debe igualmente ser valorada como prueba de cargo» y, por tanto, es «apta para desvirtuar la presunción de inocencia, sin perjuicio de que el defecto apreciado pueda afectar a su poder de convicción o fiabilidad».[185]

A pesar de que la regularidad de la cadena de custodia es un presupuesto para la valoración de la pieza de convicción obtenida, ya que es la única manera de garantizar que lo conseguido y lo que se analiza no ha sido alterado, «el incumplimiento de la misma no produce la nulidad de la prueba sino que cuestiona su autenticidad», y es en función de la relevancia que ostente la infracción cometida como se determinará la posibilidad o no de que sea valorada como prueba (STS 1072/2012 de 11 de diciembre).[186]

En materia de cadena de custodia vuelve a cobrar relevancia la firma *hash* que anotábamos en la etapa inicial del clonado, pues la integridad del contenido del dispositivo se obtiene comparando las firmas *hash* o huellas digitales que se consiguieron en la información original, que deben coincidir con lo que se presente en definitiva.

Finalmente, y a objeto de graficar con claridad el riesgo en la manipulación de las pruebas electrónicas, la doctrina española suele citar reiteradamente un fallo del Tribunal Supremo que analiza el punto, particularmente en una cuestión tan común como la mensajería instantánea. Así, la STS 300/2015, a propósito del caso en que la madre de la víctima acompaña los clásicos «pantallazos» de una comunicación bidireccional en una red social, en un caso de abuso sexual, expone que «La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparen-

---

de custodia haga «una simple reflexión genérica acerca de los riesgos potenciales de adulteración para desencadenar las dudas sobre su efectiva manipulación, con el consiguiente efecto en el ámbito del derecho a la presunción de inocencia», tal y como aduce la STS 287/2017, de 19 de abril, sino que la parte que pretenda hacer valer tal ruptura podrá proponer prueba pericial alternativa al dictamen ya elaborado por expertos y podrá designar a un experto para que esté presente durante la pericial acordada por el juez. Rodríguez (2017/2018), p. 35.

185 Considerando para estos efectos el pronunciamiento del Juzgado en lo Penal de Gijón 39/2016, de 6 de julio, citado por Rodríguez (2017/2018), pp 35-36.

186 Rodríguez (2017/2018), p. 36.

tar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido».

El punto también es importante porque nos sitúa en el extremo de este proceso, cual es la pericia informática. La doctrina del Tribunal ha permitido colegir que no en todos los casos de aportación de prueba electrónica esta será necesaria, pero, cuando se produce una impugnación en torno a la autenticidad de esta prueba, el efecto que se produce es el *desplazamiento de la carga de la prueba*, de modo que toca acreditar la misma a quien pretende beneficiarse procesalmente de los antecedentes aportados. Ahora bien, ello será necesario en caso de que la introducción de la evidencia sea hecha en virtud de mecanismos tan clásicos como febles, como una transcripción o «pantallazo», sin embargo, cuando hemos transitado a la firma del *hash*,[187] y hemos acompañado el dispositivo mismo y no solo una imagen, ya podríamos haber dotado a la información contenida en el dispositivo de la autenticidad necesaria que podría hacer que el tribunal, en su facultad de valoración de la prueba, prescinda de la pericia para efectos de establecer el hecho específico.

No existiendo mucha jurisprudencia en Chile que permita extraer principios generales en la rendición de la prueba, volvemos a citar la sentencia dictada por el Tribunal de Juicio Oral en lo Penal de Rancagua, dictada en causa RUC 1901349868-K por delito de espionaje informático y apropiación indebida, en la que el tribunal, al fundamentar su absolución excluyendo la participación de los acusados, dispone lo siguiente:

Décimo cuarto: falta de participación. Que, no se rindió probanza alguna destinada a acreditar que los acusados vulnerando el sistema de seguridad del Banco o las medidas de seguridad de la víctima fueron quienes realizaron las transacciones reclamadas. No se pesquisó la hue-

187 En Sánchez (2016), pp. 27 y ss., se alude al tránsito desde el «pantallazo» al uso del *hash*, sobre la base de la necesidad de certeza que requiere la evidencia digital, que exige mayores estándares al interior del proceso.

lla informática de la transacción para determinar cómo se realizó, de qué manera se vulneró el sistema, desde qué computador o lugar geográfico se realizó esta operación ilícita. *En definitiva, no existió absolutamente ninguna actividad probatoria por parte del ente persecutor en torno a acreditar de algún modo pericial o técnico informático que fueron los acusados quienes realizaron algún acto (como interceptar, interferir o acceder) que les haya permitido acceder a la cuenta de la víctima y realizar transacciones sin su consentimiento y depositar dinero en cuentas que se encontraban a sus nombres, apropiándose de estos.* El Ministerio Público funda su imputación en el hecho de que las cuentas en que se recibieron los fondos sustraídos estaban a nombre de los acusados, sin embargo, este hecho no es razón suficiente para dar por establecido que estos fueron quienes realizaron la operación informática que terminó en la sustracción, no pudiendo descartarse que esta apertura de cuenta haya sido obra de terceras personas que utilizaron estas cuentas como puente para la sustracción, más cuando no se realizó actividad investigativa pericial informática para acreditar o descartar este punto (énfasis añadido).

Lo cierto es que el pronunciamiento del tribunal en este caso es bastante categórico en cuanto reprocha al persecutor la ausencia de actividad probatoria cuando le corresponde, por cierto, la carga procesal, pero permite igualmente observar un mínimo estándar al exigir «algún modo pericial o técnico informático», o aludir al concepto de «huella informática de la transacción».

3.3. Regulación de la actividad probatoria en el Convenio de Budapest

El Convenio de Budapest, como se ha adelantado, contiene una amplia regulación de los aspectos procesales asociados no solo a los delitos informáticos, sino a todo delito cometido por medios informáticos y a la obtención de pruebas electrónicas de cualquier delito.[188] Si bien hay

188 El artículo 14 del Convenio establece el ámbito de aplicación de las disposiciones de procedimiento de la forma siguiente:

«1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección a los efectos de investigación o de procedimientos penales específicos. 2. Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicará los poderes y procedi-

disposiciones que pueden tener una aplicación directa al interior de los Estados suscriptores, lo cierto es que su pretensión es que se regulen, al interior de los mismos, los aspectos procesales necesarios para el esclarecimiento de los hechos punibles a los que nos vemos expuestos a diario, conforme a la legislación interna, pero con pleno respeto a los derechos humanos de todas y todos.

En efecto, el Convenio pretende servir de guía para cualquier país en sus legislaciones y como marco para la cooperación internacional, buscando el equilibrio para abordar una eficaz lucha contra la ciberdelincuencia, pero con pleno respeto a los derechos humanos, de modo de lograr un entorno cibernético más seguro y respetuoso del Estado de derecho.

En tal sentido, las restricciones que puedan imponerse por la vía de medidas procesales contempladas para investigar la comisión de delitos requieren especial atención y regulación, dada la potencial afectación a garantías básicas de las personas. Debe existir certeza respecto de las consecuencias que nuestros actos pueden traer aparejadas.

Lo cierto es que el Convenio en cuestión protege los derechos humanos, pero, a la vez, interfiere con ellos, en su disfrute y goce. Así, en el seno del Consejo de Europa ha aparecido una nueva categoría de derechos humanos, surgida a propósito del uso creciente de las nuevas tecnologías, lo que puede tener un impacto y obligarnos a repensar una conceptualización de tales derechos y, en esa nueva concepción, asumimos que los Estados deben intervenir, siempre que sea necesario, para garantizar su disfrute.[189] Pero, por otro lado, los Estados también tienen

---

mientos mencionados en el párrafo 1 del presente artículo: a. a los delitos previstos en aplicación de los artículos 2° a 11 del presente Convenio; b. a cualquier otro delito cometido por medio de un sistema informático, y c. a la obtención de pruebas electrónicas de cualquier delito».

189 Resulta de importancia considerar que los delitos en el ciberespacio también pueden afectar los derechos humanos de las personas. En ese sentido, un pronunciamiento claro que suele citarse es el caso *KU c. Finlandia*, TEDH 2872/02. En este caso, se acciona contra un hombre que publicó fotos de un niño de doce años en una página de citas para hombres, con un enlace de acceso a una foto de la víctima y sus datos de contacto. Se presentó una denuncia en sede penal, pero el proveedor de servicios se negó a entregar la identidad de la persona por respeto a su confidencialidad, cuestión que fue avalada por el tribunal local. El TEDH señala en el párrafo 46 que «[…] Para el Tribunal, los Estados tienen la obligación positiva inherente al artículo 8 del Convenio de penalizar delitos contra la persona incluidos las tentativas y reforzar el efecto disuasorio de la penalización poniendo en práctica

el deber de abstenerse de injerir indebidamente en el goce de los derechos humanos, por lo que nos encontramos en la necesidad de lograr ese delicado equilibrio que nos exige el proceso penal entre el interés público en el esclarecimiento de los hechos constitutivos de delito y los derechos de las personas como sujetos pasivos de la persecución penal.

En esa difícil tarea, luego de establecer el ámbito de aplicación de las medidas procesales y las condiciones y salvaguardias como declaraciones esenciales en la actividad procesal más o menos intrusiva, el Convenio describe una serie de actividades específicas en este ámbito, que se tratan en las líneas siguientes.

A) Conservación rápida de los datos informáticos almacenados

En el Título 2 de la Sección II del Convenio se abordan dos medidas, la conservación rápida de los datos informáticos almacenados y la conservación y revelación parcial de los datos relativos al tráfico.

Para tales efectos, en el Capítulo I el instrumento se encarga de definir la terminología que se aplicará, explicando que por «datos informáticos» se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función, mientras que por «datos relativos al tráfico» se entienden todos los relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Respecto de los datos informáticos, se prevé que cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.

---

las disposiciones penales mediante la investigación efectiva y el enjuiciamiento […]. Cuando el bienestar físico y moral de un niño se ve amenazado, tal requerimiento judicial asume incluso mayor importancia».

Y que cuando un Estado aplique lo dispuesto en el párrafo 1 anterior, por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, el Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las partes podrán prever la renovación de dicha orden.

Cuando la disposición alude a la forma en que puede obtenerse la conservación, es amplia y respetuosa del derecho interno de cada Estado parte y, por ello, podría tratarse de una orden judicial o administrativa; el factor importante está asociado a la oportunidad, al sentido de urgencia, por lo que la norma alude a la agilidad en el proceso de conservación de los datos.

Es importante hacer presente que la conservación rápida apunta a que los datos existen y la obligación apunta a que pueda exigirse a una persona o entidad la protección de dichos datos respecto de cualquier circunstancia que pudiera significar una modificación, deterioro y, por cierto, eliminación de los mismos. Es decir, el espíritu de la legislación apunta a lograr que los datos se guarden de manera segura y, por tanto, significa más que una obligación de retención de la información.[190]

La norma, en todo caso, no exige el congelamiento de los datos, vale decir, que se hagan inaccesibles a terceros y, por el contrario, sería posible obtener duplicaciones o copias de los mismos a las que puedan tener acceso los usuarios legítimos.

Si bien el poder se extiende a todos los datos informáticos, como registros personales, de salud, financieros y también datos relativos al tráfico, es importante tener presente que esta medida debe estar asociada a una investigación penal en particular y que la orden, en respeto al principio de proporcionalidad, debe referirse a datos específicos y no puede tratarse de una medida que afecte a un número desproporcionado de datos.

Por otro lado, el mecanismo no apunta a una obligación general de retención de datos y se refiere a datos que estén disponibles y sean objeto actual de almacenamiento por una persona o entidad. En definitiva,

190 Bosch (2018), pp. 124-141.

es posible que los datos no puedan ser materia de almacenamiento por capacidad presupuestaria, técnica o la razón que fuere, y ello no es sancionado jurídicamente.

Ahora, para que tenga lugar la orden de conservación rápida, la norma discurre sobre el supuesto de que existan motivos para creer que los datos *son particularmente susceptibles de pérdida o de modificación.* No hay ejemplos de esta circunstancia, pero debemos partir de la base de que prácticamente todos los datos se encuentran en esta situación, por lo que probablemente el espíritu apunta a encontrarnos en un estadio superior en cuanto a las sospechas sobre la persona responsable de los datos, las inseguras condiciones de almacenamiento o las drásticas políticas de supresión de datos, conforme a la normativa imperante en materia de protección de datos personales en un Estado determinado.

Con la referencia a que se encuentren en poder o bajo el control de esa persona, se alude a que esta tenga la posesión física de los datos, o bien, a que tenga la posesión constructiva, esto es, que tenga libre control sobre su presentación, pero no se incluye la capacidad técnica de acceder remotamente a datos que no estén bajo el control legítimo de la persona.

Se trata de una medida esencialmente temporal: la duración de la misma debe estar especificada en la orden y no puede ser, en caso alguno, superior a los noventa días. Debemos considerar que se trata de una medida instrumental a otra: obtener, por parte de la judicatura, las autorizaciones correspondientes para medidas más invasivas, como lo sería una orden de presentación o para un registro y confiscación.

Finalmente, la normativa obliga a cada Estado a adoptar las medidas legislativas y de otro tipo que resulten necesarias para compeler a la persona que custodia los datos o a la encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno. Lo anterior cumple varias finalidades y parte del reconocimiento de la calidad de preliminar de esta primera medida tratada por el Convenio. Primero, hay derechos de personas comprometidas que merecen el respeto a su privacidad y, por cierto, existe la necesidad de velar por el éxito investigativo, de modo que se precisa que tanto los involucrados como cualquier persona que pueda tener acceso a los datos no entorpezcan las labores de esclarecimiento.

B) Conservación y revelación parcial rápidas de los datos relativos al tráfico

Esta medida, si bien va un paso más allá y alude no solo a la conservación, sino también a la revelación parcial de información, recae en un objeto distinto: los datos relativos al tráfico. No reiteraremos la definición que se ofrece al inicio del Convenio, pero sí es importante señalar que los datos relativos al tráfico no incluyen el contenido de la comunicación, sino solo los relativos a aspectos como día, fecha, hora, duración, tamaño, tipo de servicio, entre otros.

La disposición señala que, con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para a) garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación, y b) asegurar la revelación rápida a la autoridad competente del Estado, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicho Estado pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido.

Ocurre que lo normal en la transmisión de comunicaciones es que intervengan distintos proveedores de servicio que muchas veces comparten los datos de tráfico entre sí, por razones de seguridad, técnicas, comerciales, etc. Así, la regla es que los proveedores de servicio no cuenten con todos los antecedentes que les permitan determinar el origen y destino de una comunicación y, por el contrario, dispongan de información parcial.

Por eso este poder no se limita a la conservación, sino que apunta a la revelación rápida de los datos relativos al tráfico que permita identificar a otros proveedores de servicio implicados en la transmisión de la comunicación y la vía por la cual esta se ha hecho. El objetivo, entonces, es identificar a todos los proveedores de servicio para adoptar las medidas procesales que sean útiles en el caso concreto.

Sin esta medida, se dice, la fiscalía tomaría conocimiento de otras empresas proveedoras de servicios (que fueron parte de la transmisión de la comunicación y que tienen información necesaria para rastrearla) únicamente una vez que la información conservada por la primera empresa requerida sea puesta a disposición del Ministerio Público, previa

autorización judicial. Para esa época, las otras empresas podrían ya haber eliminado los datos; de allí la utilidad de esta disposición.[191]

Si bien en este caso y, a diferencia del anterior, la medida no incluye solo la orden de que se conserven datos, sino también que estos se revelen parcialmente, no se trata de una facultad intrusiva, porque implica únicamente la revelación de los datos relativos al tráfico –no su contenido– y en forma limitada.

C) Orden de presentación

El artículo 18 dispone que cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a) a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático, y b) a un proveedor que ofrezca sus servicios en el territorio de dicho Estado, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios.

Como en todos los casos, luego establece las exigencias mínimas de salvaguardia y legalidad, remitiéndose a los artículos 14 y 15, y posteriormente explica lo que debe entenderse por «datos relativos a los abonados», aludiendo a cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar a) el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio; b) la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio; y c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

En primer lugar, cabe advertir que la norma se refiere a cualquier persona presente en el territorio de ese Estado, incluyendo a un provee-

191 *Ídem.*

dor de servicios, pero no alude al lugar donde los datos se encuentren ubicados, que podrían estar en un sitio distinto.

En cuanto a los datos, alude a ellos sin distinción, pero sí resulta relevante considerar que debe tratarse de datos específicos y no de una cantidad indiscriminada de los mismos, cuestión que deberá estar especificada en la orden respectiva. En tal sentido, se podría ordenar la presentación de una dirección de correo electrónico asociada a un nombre determinado; en cambio, no sería admisible que se ordenara la presentación de todas las comunicaciones recibidas en esa cuenta de correo electrónico durante los últimos cinco años.

Respecto de la referencia a que estén en poder o bajo el control de una persona, reiteramos lo dicho a propósito de la conservación, esto es, puede tratarse de una posesión física o una posesión constructiva, pero no incluye la facultad de acceder remotamente a datos que no estén bajo el control legítimo de esa persona.

Tampoco esta medida obliga a las personas o entidades a retener datos y se refiere únicamente a los datos almacenados, vale decir, existentes en su poder conforme a la explicación previa.

En lo que respecta al proveedor de servicios, no es necesario que este esté presente en el territorio del Estado, sino que basta que ofrezca sus servicios en el mismo; por tanto, si el proveedor de servicios permite a los habitantes de ese Estado contratar sus servicios, emite publicidad para tales efectos o interactúa de otra forma con los abonados en ese ámbito local, lo encontraremos incorporado en la norma.

Este requisito se grafica con el denominado caso de la *Fiscalía belga contra Yahoo*, que duró seis años, a contar de 2009. Se trató de una investigación llevada a cabo por estafas informáticas en las que los sujetos compraban equipos de alta tecnología en línea con tarjetas de crédito fraudulentas y utilizaban sus direcciones de correo electrónico de Yahoo. Si bien esta última no tenía un punto de contacto físico en Bélgica, la fiscalía concluyó que, dado que la víctima era belga, el delito había sido cometido en Bélgica, la fiscalía competente era la de Bélgica y la empresa proveedora de servicios tenía *presencia judicial en Bélgica*, por cuanto ofrecía sus servicios en ese país, lo que podía acreditarse por el idioma utilizado en sus anuncios, por noticias regionales que transmitía, por los servicios dirigidos con *banners* comerciales con publicidad dirigida basada en *cookies*, quedaba demostrado que Yahoo había elegido voluntariamente someterse a la jurisdicción belga en el momento

en que decidió hacer virtualmente negocios en ese país. Por ello, lo que correspondía era una orden de presentación y no un requerimiento de asistencia jurídica a Estados Unidos, país de origen de la empresa. Lo anterior, como podrá preverse, no era aceptado por la empresa, que señalaba que Bélgica no tenía jurisdicción a su respecto, porque eso solo cabía a Estados Unidos, de modo que lo que correspondía era una solicitud de asistencia internacional. Por tal motivo, se negó a la presentación, lo que implicó que se le procesara por el incumplimiento del deber de cooperación que, de acuerdo con la legislación belga, es un delito.[192]

Tras varios años de litigio en diversas instancias judiciales, la justicia belga, a través del Tribunal de Casación, condenó a Yahoo razonando sobre la base de que, en el caso concreto, no nos encontrábamos ante una situación de jurisdicción extraterritorial, ya que Yahoo debía considerarse presente en Bélgica en consideración a que voluntariamente accedió someterse a su jurisdicción cuando ofreció sus servicios en dicho país, de modo que lo que correspondía era una medida del derecho interno como la orden de presentación; en cambio, no correspondía ningún acto sustantivo en otro país, como sería una solicitud de asistencia internacional remitida a los Estados Unidos.

Los datos relativos a los abonados pueden ser de cualquier forma, vale decir, informáticos o no, entre los que podemos encontrar cuestiones de carácter técnico asociadas al servicio, el mismo tipo de servicio de que se trata, como datos personales referidos a la identidad, número de teléfono y datos relativos al pago de los servicios contratados.

Como la empresa prestadora de los servicios puede estar localizada en el extranjero y solo ofrecer sus servicios en el territorio de ese Estado, así como puede hacerlo en otros territorios, es importante tener presente que la orden de presentación únicamente puede referirse a los servicios que presta en el territorio de ese Estado requirente, y no podría referirse a abonados o a situaciones existentes en el territorio de otro Estado.

Un ejemplo entre varios que podríamos encontrar en esta materia es Facebook, de modo que cualquier Estado podría pedirle la presentación de datos, puesto que ofrece sus servicios prácticamente en todo el globo.

192 Elmundo.es (2009), s.p.; La Vanguardia (2009), s.p.; El País (2011), s.p.

D) Registro y confiscación de datos informáticos almacenados

Avanzando en el Convenio vamos encontrando medidas cada vez más intrusivas, y así es como el artículo 19 contempla el registro y la confiscación de los datos informáticos almacenados, en consideración a que la orden de presentación no siempre será la medida adecuada; por ejemplo, no lo es cuando quien posee o controla los datos informáticos es precisamente el blanco de la investigación. En tal sentido, esta norma señala que deben adoptarse, en cada Estado, las medidas necesarias para que las autoridades competentes puedan registrar o tener acceso de un modo similar a todo sistema informático o parte del mismo, así como a los datos informáticos almacenados en él y a todo dispositivo de almacenamiento informático que permita almacenar datos, en su territorio.[193]

193 Artículo 19: «Registro y confiscación de datos informáticos almacenados
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de un modo similar:
a. a todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados, y
b. a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio.
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurarse de que, cuando, de conformidad con el apartado 1.a), sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 o 2.
Estas medidas incluirán las siguientes prerrogativas:
a. confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento informático;
b. realizar y conservar una copia de esos datos informáticos;
c. preservar la integridad de los datos informáticos almacenados pertinentes, y
d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado.
4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para

En primer lugar, la norma alude a *registro* y con ello entendemos que se faculta la realización de un examen, revisión o inspección. Sin embargo, también anota un *acceso de modo similar*, situación contemplada para adoptar una terminología que fuera tecnológicamente neutra, que permitiera revisar datos intangibles que puedan encontrarse en algún formato electromagnético.

El objeto de la medida es bastante amplio, pues ella puede apuntar a todo un sistema informático, a una parte del mismo, a los datos informáticos almacenados en un sistema informático y a todo dispositivo de almacenamiento informático que permita almacenar datos en su territorio.

Para poder *extender* el registro o el acceso de un modo similar, conforme al numeral 2 de la norma, se requiere copulativamente lo siguiente:

- Que existan motivos para creer que los datos buscados se encuentran en ese sistema informático o en una parte del mismo.
- Que el otro sistema informático o la parte de él también se encuentre en territorio del Estado requirente, o bien los datos objeto de extensión son legítimamente accesibles desde el sistema informático inicial.

Todo ello sin perjuicio de que la extensión pueda estar, conforme al derecho interno, sujeta a exigencias adicionales, como la necesidad de autorización judicial.

En cuanto a confiscar, el término alude a la actividad de incautar, requisar, embargar, de forma tal que nos encontramos con una actividad mucho más invasiva que las anteriores, donde es el propio dominio el que puede encontrarse afectado.

En cuanto a la expresión «obtener de un modo similar», insistimos en que con ello pretende aludirse a actividades similares, pero con un contenido informático que puede no quedar amparado por el término «confiscar».

No obstante lo anterior, y pese a su sentido natural y obvio, la confiscación no siempre supone la actividad de tomar físicamente el sistema informático o el dispositivo de almacenamiento; podría perfec-

---

proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2».

tamente hacerse una copia de los datos, puesto que lo importante es el contenido, por lo que es una alternativa a evaluar en cuanto a que podría resultar menos onerosa que la que implica asumir la responsabilidad de protección de todos los datos, en algún caso concreto.

El estándar necesario para la autorización judicial de la medida debiera ser equivalente, en nuestro país, al que se impone a la fiscalía para solicitar las diligencias de entrada y registro e incautación de evidencia, por la naturaleza de la diligencia.[194]

La norma menciona la necesidad de preservar la integridad de los datos informáticos almacenados pertinentes y con ello no hace otra cosa sino aludir a la necesidad de resguardar la cadena de custodia, en los términos referidos en el acápite anterior. Se trata de tomar todas las medidas necesarias para asegurar que lo confiscado en un momento dado sea exactamente lo mismo que posteriormente será analizado y eventualmente presentado en un juicio oral.

Luego, la disposición también establece la prerrogativa de hacer inaccesibles o suprimir los datos informáticos del sistema informático consultado, objetivo que podría lograrse mediante la aplicación de cualquier medida técnica apta para tales efectos, como podría ser una técnica de cifrado. Ello tendrá lugar cuando se trate de datos que resulten peligrosos en su formato original, por lo que se hace necesario ocultarlos, como podría ocurrir si nos encontramos ante material pornográfico infantil.

Finalmente, el artículo 19 establece la posibilidad de que se ordene a cualquier persona que conozca el funcionamiento de un sistema informático, o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir el registro descrito. Ello puesto que muchas veces resulta necesario, o al menos conveniente, consultar a los administradores de los sistemas respecto de las mejores formas de realizar el registro o requerirles que proporcionen alguna clave de acceso. Esto, por un lado, puede ser un aspecto favorable para la propia empresa, en términos de su colaboración con las fuerzas de orden y seguridad, y, por otro, permite dotar de mayor eficacia a la medida. Por cierto, todo ello en cuanto no se comprometa injustificadamente la privacidad de las personas y se encuentre en el marco de lo razonable.

194 *Ídem*.

E) Obtención en tiempo real de datos relativos al tráfico

Hasta el registro y confiscación contemplados en el artículo 19, todas las medidas revisadas se referían a *datos almacenados*; sin embargo, el Título 5 ya discurre sobre la base de la obtención en *tiempo real* de los datos, ya sea relativos únicamente al tráfico, ya sea de aquellos con contenido propiamente tal, es decir, datos que se encuentran en tráfico o circulación.

El artículo 20 se refiere a los datos relativos al tráfico[195] y otorga tres facultades a la autoridad competente, consistentes en 1) obtener o grabar directamente los datos relativos al tráfico; 2) obligar a una empresa proveedora de servicios a obtener o grabar los datos relativos al tráfico, o 3) obligar a una empresa proveedora de servicios a colaborar o asistir a esa autoridad en la obtención o grabación de los mismos datos relativos al tráfico.

En cuanto a la forma, medio o modalidad de obtener o grabar los datos relativos al tráfico, la normativa no establece limitaciones, por lo que se hará por el medio técnico que resulte idóneo para lograr la finalidad prevista, vale decir, existe neutralidad tecnológica en la regulación, pero

195 Artículo 20: «Obtención en tiempo real de datos relativos al tráfico
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes:
a. a obtener o grabar con medios técnicos existentes en su territorio, y
b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:
i. a obtener o a grabar con medios técnicos existentes en su territorio, o
ii. a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15».

siempre atendiendo a las capacidades técnicas propias de la proveedora de los servicios, esto es, no se les impone obligación alguna en torno a desarrollar capacidades inexistentes en su organización, ni que puedan ver sus costos encarecidos con contrataciones de expertos, adquisición de equipamientos específicos ni desarrollos ajenos a sus capacidades rutinarias.

Esta disposición también limita la aplicación a datos específicos sin que se conciba una autorización para la obtención o grabación indiscriminada de datos, conforme al equilibrio por el que procura velar el Convenio en torno a los derechos y garantías involucrados en la ejecución de las medidas.

Por otra parte, también existe una limitante espacial, por cuanto la medida puede adoptarse respecto de comunicaciones que se desarrollen dentro del territorio del Estado respectivo. Ahora bien, se entiende que se puede obligar al proveedor de servicios si cuenta con una infraestructura física en el territorio del Estado de que se trate, aun cuando no esté allí su oficina central. Si una de las partes que se comunica, entendiendo por tal no solo a la persona física, sino también al equipo, o bien el equipo informático se encuentra dentro del territorio del Estado que está expidiendo la orden, se entiende que se cumple con el requisito.

El párrafo 2° establece que "Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio», por cuanto algunos países no permiten la medida sin que a lo menos exista un conocimiento de la diligencia por parte de la empresa proveedora de servicios, con lo cual, alternativamente, para estos casos se contempla la referida solución.

Como resulta bastante lógico a la luz de la eficacia de la medida, se contempla la necesaria confidencialidad o secreto que puede imponerse respecto de la operación, a fin de que no se entorpezca la investigación.

F) Interceptación de datos relativos al contenido

Finalmente, esta norma contiene la medida más intrusiva de toda la regulación, a la vez que probablemente unas de las más útiles, que se

refiere a la interceptación de los datos relativos al contenido[196], es decir, permite la obtención en vivo del contenido de las comunicaciones que se están sosteniendo. Considerando que se trata de la medida más lesiva que puede existir en la legislación interna de cada país, debiera contemplarse el mayor estándar posible para su procedencia, comenzando por la gravedad de las conductas ilícitas que la hacen procedente, es decir, solo debería ser posible su adopción tratándose de los delitos más graves que se contemplen en cada ordenamiento.

Sobre la base, entonces, de ese estándar de procedencia más exigente, atendida la mayor intromisión en la intimidad de las personas, la medida de interceptación de contenido en tiempo real faculta a la autoridad competente para 1) obtener o grabar directamente los datos relativos al contenido; 2) obligar a un proveedor de servicios a obtener o grabar los datos relativos al contenido, o 3) obligar a una empresa proveedora de servicios a colaborar o asistir a esa autoridad en la obtención o grabación de los mismos datos relativos al contenido.

Al igual que en el caso anterior, no existen limitaciones respecto de la modalidad técnica de obtención de los datos relativos al contenido, pudiendo esta ser la compatible, disponible o adecuada al escenario con-

196 Artículo 21: «Interceptación de datos relativos al contenido
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno a:
a. obtener o grabar con medios técnicos existentes en su territorio, y
b. obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a:
i. obtener o grabar con medios técnicos existentes en su territorio, o
ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar, en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio con medios técnicos existentes en ese territorio.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15».

creto, y sin que, en el caso de requerirse apoyo o que se exija el mismo a la proveedora de servicios, ello implique para esta algún encarecimiento de sus costos por exigencias superiores.

La diferencia con el caso anterior dice relación con el contenido, pues precisamente es esta la diligencia que apunta al conocimiento mismo de la comunicación, al contenido comunicativo y no únicamente de los datos de los comunicantes. Es el mensaje mismo, la finalidad de lo transmitido, a lo que se puede acceder a partir de esta medida. Por ello, y con mayor razón, rigen las limitaciones en cuanto a la extensión de la medida, de modo que debe tratarse de comunicaciones específicas sin que sea admisible que se trate de un tratamiento indiscriminado de las comunicaciones sobre las que recae la medida.

En todo lo demás aplican las mismas disposiciones que respecto de la medida relativa a la obtención en tiempo real de los datos relativos al tráfico, vale decir, las limitaciones en cuanto al territorio del Estado respectivo, los límites que puedan existir en el derecho interno que lleven a la necesidad de adoptar una conducta diferenciada con el proveedor del servicio, y, por cierto, lo relativo a la obligación de secreto respecto de la diligencia, absolutamente indispensable para la utilidad de la misma.

Esta interceptación contiene la única disposición del Convenio que incluye una limitación explícita en cuanto al principio de proporcionalidad, toda vez que establece la medida únicamente para el caso de delitos graves, teniendo en cuenta la afectación a la vida privada de las personas.[197]

Ahora, respecto de cada una de las medidas contempladas entre los artículos 16 y 21 del Convenio rigen, según lo establecido en el inciso final de cada una de las disposiciones, a modo de reiterar la disposición general descrita en norma previa, las *condiciones y salvaguardias* dispuestas en el artículo 15.[198]

---

197 *Ídem*.

198 Artículo 15: «Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales

Se trata de una norma esencial a la hora de obtener ese delicado equilibrio que debe existir entre la necesidad de asegurar un entorno cibernético libre de delincuencia, que permita el goce de los derechos fundamentales, y, a la vez, respetar esos mismos derechos cuando se trate de hacer injerencias necesarias en los mismos con la finalidad de lograr el objetivo anterior. Ahora bien, lo que el texto del Convenio hace es una declaración, que reitera en cada medida, pero dejando la determinación de su contenido a lo que contemple el derecho interno de cada Estado.

En definitiva, lo que la norma pretende es relevar la importancia del respeto al principio de proporcionalidad en todas estas investigaciones, aunque, insistimos, confiándolo a las legislaciones propias de cada país.[199]

De modo ilustrativo, sí contempla algunas referencias, como la necesidad de control, pero sin que este control quede únicamente limitado a la vía judicial, sino que disponible también para supervisiones de carác-

---

aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Parte examinará los efectos de los poderes y procedimientos mencionados en la presente Sección sobre los derechos, responsabilidades e intereses legítimos de terceros».

199 Un pronunciamiento importante en materia de principio de proporcionalidad es el contenido en el caso *Soering contra Reino Unido*, TEDH 14038/88, que en su considerando 89° dispone que «La calificación de 'penas o tratos inhumanos o degradantes' depende del 'conjunto de las circunstancias del caso' (apartado 100, posterior). Además, *la preocupación por asegurar un equilibrio justo entre las exigencias del interés general de la sociedad y los imperativos de la protección de los derechos fundamentales de la persona es inherente al conjunto del Convenio.* La facilidad con que hoy se viaja por todo el mundo y el aumento de la delincuencia internacional hace que todas las naciones tengan un interés creciente en que se pongan a disposición de la justicia los presuntos delincuentes que huyen al extranjero. A la inversa, la creación de asilos o refugios para fugitivos no solo supondría un peligro para el Estado obligado a acoger a la persona protegida, sino que socavaría también los fundamentos de la extradición. Hay que incluir estas consideraciones entre los factores que deben tenerse en cuenta para interpretar y aplicar, en materia de extradición, los conceptos de pena o de trato inhumano o degradante. Artículo 3 (Prohibición de sometimiento a tortura y a penas o tratos inhumanos o degradantes)».

ter administrativo (dependiendo de cada ordenamiento), o limitaciones referidas a la vigencia de la medida y la exigencia más alta respecto de su concurrencia. Básicamente son cuatro las salvaguardias mínimas que se exigen en el Convenio: 1) supervisión judicial u otra forma de supervisión independiente; 2) motivos que justifiquen su aplicación; 3) limitación del ámbito de aplicación, y 4) duración de dicho poder o procedimiento.

El Tribunal Europeo de Derecho Humanos aporta bastante jurisprudencia en lo que respecta a la afectación de los derechos fundamentales que se produce en el marco de investigaciones penales por delitos informáticos, o mediante la obtención de evidencia digital, analizando si se cumplen las condiciones de salvaguardia que exige la proporcionalidad.

Por ejemplo, en 2017, en *Trabajo Rueda contra España* se consideró que la confiscación del computador del imputado en un caso que involucraba tenencia de material de abuso sexual infantil, fue desproporcionada e innecesaria en una sociedad democrática, por el hecho de que el registro careció de una autorización judicial previa.[200]

En *Szabó y Vissy contra Hungría*, en 2016, el Tribunal estimó que no se cumplía con las salvaguardias y no había garantías suficientes contra los abusos, pero, en este caso, por parte de la legislación, que permitía la adopción de medidas electrónicas de vigilancia, registro e interceptación de comunicaciones por orden del ministro de Justicia y sin autorización judicial, por lo que el tribunal estimó que el hecho de que la supervisión estuviera a cargo de un miembro del Ejecutivo, políticamente responsable, no ofrecía garantías suficientes.[201]

El equilibrio que se busca debería incluir la minimización en la interrupción de servicios de los consumidores, exención o atenuación de responsabilidad en caso de cooperación y salvaguarda de intereses patrimoniales, en la medida de lo posible.

G) Jurisdicción

Si bien no se trata de un aspecto probatorio, la última disposición que el Convenio contempla dentro de la sección procesal es la relativa a un aspecto de suma relevancia, como lo es el relativo a la jurisdicción. Se trata de un aspecto orgánico, no funcional, que suele ser de fácil despa-

200 *Trabajo Rueda contra España*, TEDH 32600/12, 30 de mayo de 2017.
201 *Szabó y Vissy contra Hungría*, TEDH 37138/14, 12 de enero de 2016.

cho en distintas materias, pero que, cuando hablamos de ciberdelitos o, incluso, de pruebas electrónicas, cobra un vigor fundamental, dado que se trata de dos situaciones que no reconocen muchas fronteras, pero estas siguen existiendo para los Estados, sobre todo en un tema relevante en términos de soberanía como lo es la jurisdicción.

El artículo 22 del Convenio dispone que cada Estado adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2° a 11 del presente convenio, cuando el delito se haya cometido:

a) en su territorio; o
b) a bordo de un buque que enarbole su pabellón; o
c) a bordo de una aeronave matriculada según sus leyes; o
d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

Dispone también que los Estados podrán reservarse el derecho a no aplicar, o a aplicar solo en determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier parte de dichos apartados, *como ocurre en el caso de Chile*.[202]

Luego, que cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito mencionado en el párrafo 1 del artículo 24 del presente Convenio cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de su nacionalidad, previa demanda de extradición.

Posteriormente declara que el Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno y que, en el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción

202 Reservas al Convenio sobre la Ciberdelincuencia: «d) La República de Chile expresa, de conformidad al artículo 22, párrafo 2, del Convenio sobre la Ciberdelincuencia, que no aplicará las normas sobre jurisdicción establecidas en el apartado 1 d. del mismo artículo».

penal.[203] En tal sentido la norma dispone que: «5. En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal».

Al respecto, un pronunciamiento importante fue dictado por la Audiencia Provincial de Las Palmas de Gran Canaria, en orden a interpretar la norma en el sentido de introducir un criterio de conveniencia para decidir respecto del tribunal que conocerá de los hechos, de la forma siguiente: «[…] En definitiva, declara el alto Tribunal 'en los delitos informáticos, el criterio de la eficacia en la instrucción desplaza a la teoría de la ubicuidad'. Por eso aunque Tarancón comenzó a actuar antes y allí reside el perjudicado, habiéndose cometido en su territorio el elemento del delito del desplazamiento patrimonial, la competencia debe dirimirse en favor de Ceuta y por último decir que a la misma conclusión se llegaría si tuviéramos en cuenta el *criterio de la mayor facilidad y conveniencia en la investigación*, también utilizado por nuestra jurisprudencia, y mantenido en este tipo de delitos por el Convenio sobre el Cibercrimen, suscrito en Budapest el 23 de noviembre de 2001, ratificado por España el 27/09/10, que determina que será competente el Estado 'que esté en mejores condiciones para ejercer la persecución del delito' (artículo 22.5) […] (énfasis añadido). En aplicación de este criterio baste señalar que resulta que este fuero territorial era el más adecuado para conocer de los hechos. En todo caso, las dudas nunca conducirán a la nulidad de la sentencia, pues no se produce indefensión alguna del recurrente, mucho menos cuando ni siquiera fueron alegadas en el momento procesal oportuno".[204]

---

203 Un interesante análisis en esta materia se ofrece en Cárdenas (2008), pp. 1-14. Aquí la autora analiza críticamente la extensiva interpretación que se ha hecho del principio de territorialidad en materia de cibercriminalidad, al punto de llegar a entenderse que cualquier Estado puede reclamar jurisdicción para conocer de estos delitos. Señala que «Cierto es que la detección, persecución y castigo del denominado cibercrimen tiene particularidades que lo hacen particularmente complejo. Tanto así, que se aventura decir que el sistema de justicia criminal que se aplique no tendrá impacto en el cibercrimen, por las bajas probabilidades que hay en cuanto a su detección, persecución y esperanza de castigo. Empero, el sistema no se hace mejor si los ajustes que se llevan a cabo para su mayor eficacia dejan de lado la salvaguarda de ciertas garantías fundamentales».

204 Causa Rol 1109/18, sentencia 000173/2019, de la Audiencia Provincial de Las Palmas.

3.4. Regulación de la actividad investigativa y probatoria en la legislación chilena interna

Como anticipamos, la legislación interna de la Ley 21.459 no es abundante en normas procesales y medidas investigativas. Concretamente, podemos ver que esta ley regula la materia en su artículo 12 y en la modificación que introduce al Código Procesal Penal, incorporando el artículo 218 bis. Sin embargo, producto de ulteriores modificaciones legislativas, el estado actual de la normativa procesal procura una aproximación importante a la normativa contenida en el Convenio. Pasaremos, entonces, a revisar estas disposiciones.

A) Interceptación de comunicaciones

El artículo 12 dispone que, cuando la investigación de los delitos contemplados en los artículos 1°, 2°, 3°, 4°, 5° y 7° de la LDI lo hiciere imprescindible y existieren fundadas sospechas, basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en los preceptos precedentemente señalados, el juez de garantía, a petición del Ministerio Público, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas. Es decir, la medida se amplía respecto de su marco general, previsto a partir del artículo 222 del CPP, a los tipos penales contemplados en la normativa, con la sola excepción de la receptación de datos informáticos (artículo 6°) y el abuso de los dispositivos (artículo 8°), lo cual es muy importante porque se trata de la medida más invasiva respecto del derecho a la intimidad que contempla nuestra legislación y, consecuentemente con ello, exige el mayor estándar posible para efectos de su procedencia.[205] Este estándar se encuentra fijado por las fundadas sospechas, basadas en hechos determinados, de que una persona ha cometido o participado en la preparación o comisión, o que ella prepara actualmente la comisión o participación de los delitos previamente enunciados, sin que importe en este caso, a diferencia de lo que ocurre en materia general, la pena asignada al delito o, dicho de otro modo, independientemente de que esta no alcance el umbral de pena de crimen normalmente exigido.[206]

205 En tal sentido, Horvitz y López (2003), pp. 527 y ss.

206 Misma solución utilizada en otras categorías delictivas, como ocurre en materia de la Ley 20.000.

Para los efectos de solicitar la autorización, el Ministerio Público deberá presentar un informe previo detallado respecto de los hechos y la posible participación y, concedida la autorización por parte del órgano jurisdiccional, resultan aplicables supletoriamente todas las medidas contempladas en los artículos 222 a 226 del CPP. De este modo, no solo puede decretarse la interceptación de comunicaciones, sino también el registro remoto de equipos informáticos (artículo 225 bis) y otros medios técnicos de investigación consistentes en el empleo de medios tecnológicos para captar, grabar y registrar subrepticiamente imágenes o sonidos en lugares cerrados o que no sean de libre acceso al público, cuando existan fundadas sospechas, basadas en hechos determinados y graves, que lo hagan imprescindible para el esclarecimiento de los hechos.

La orden que disponga la realización de estas técnicas deberá indicar circunstanciadamente el nombre real o alias y dirección física o electrónica del afectado por la medida y señalar el tipo y la duración de la misma. El juez podrá prorrogar la duración de esta orden, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en el inciso precedente.

Estas técnicas de investigación resultan fundamentales para el esclarecimiento de esta clase de delitos, en los que la vulnerabilidad y volatilidad de los datos hace particularmente importante contar con evidencia obtenida en tiempo real. Así, en este caso, no es que se pase por alto el respeto al principio de proporcionalidad con relación a la pena asignada a los delitos, sino que, puesta en la balanza la eficacia de los medios necesarios para esclarecer las conductas delictivas, prevalece por sobre la afectación de derecho que trae aparejada la medida.

Recordemos que el principio de proporcionalidad también se ve reflejado en las importantes exigencias que implica la concesión de la medida por parte del órgano jurisdiccional, si bien no en cuanto a la pena asignada al delito, sí en cuanto a los requisitos que deben cumplirse para justificar la medida. Además, la legislación contempla las salvaguardas que ordena el Convenio de Budapest cuando establece los requisitos de la resolución que autoriza la medida (artículo 225 ter) y las exigencias para efectos de ampliación del registro (artículo 225 quáter).

Una norma muy importante, coherente con lo que establece el Convenio de Budapest, es la que contempla el artículo 225 quinquies, relativa al deber de colaboración impuesto sobre los prestadores de servicios

de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información y los titulares o responsables del sistema informático o contenido objeto del acceso remoto, quienes estarán obligados a colaborar con los funcionarios policiales encargados de ejecutar la medida. Asimismo, estarán obligados a facilitar la asistencia necesaria para que los contenidos aprehendidos puedan ser objeto de examen y visualización. Luego de imponerles estos deberes, la ley los obliga a guardar secreto respecto de las diligencias, con la sola salvedad de que se les cite a declarar.

En efecto, este aspecto es de suma relevancia en materia de ciberdelincuencia y pruebas electrónicas, en que necesitamos a los proveedores de servicio para acceder a los datos y la información disponible. Pero lograr la colaboración de las empresas proveedoras de servicio no es fácil porque estamos en el delicado ámbito de nuestra privacidad, la que valoramos y a la que otorgamos el estatus de derecho fundamental. Así las cosas, entonces, para los proveedores de servicios no aparece como una alternativa seductora presentarse como un asistente o apoyo a las fuerzas de orden y seguridad, que pueden lesionar ese derecho fundamental. Ello es bastante paradójico, porque lo que las personas entregamos diariamente a Internet probablemente es superior a muchas de las repercusiones o vulneraciones a la intimidad que podamos tener en el marco de una investigación penal. Como sea, se trata, junto con la transnacionalización, de una de las complejidades de la persecución penal de este tipo de ilícitos, por lo que el hecho de que se haya introducido una disposición que tienda a hacerse cargo del problema amerita un reconocimiento, independientemente de los resultados de esta colaboración, lo que seguramente requerirá mucho más que la sola dictación de la norma y precisará la generación de alianzas y, previo a ello, la necesaria sensibilización y concientización en cuanto a lo indispensable que resulta hacer esfuerzos conjuntos que permitan conseguir los objetivos perseguidos.

B) Agente encubierto

De un modo que supera el Convenio, el inciso final del artículo 12 de la LDI establece la posibilidad de utilizar un agente encubierto. Del texto de la norma surge la duda de cuál es el estándar para la procedencia de la medida, por cuanto el inciso final remite al inciso anterior para efec-

tos de la procedencia, pero el inciso anterior no alude al estándar, sino únicamente a los requisitos que debe contener la resolución que ordena la medida. Entonces, podemos entender que la referencia está hecha al inciso primero, de modo que sería la misma exigencia que la establecida para las medidas anteriores, esto es, fundadas sospechas basadas en hechos determinados de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en los artículos 1°, 2°, 3°, 4°, 5° y 7° de la ley y la investigación lo hiciere imprescindible. O, por el contrario, deberíamos entender que existe una amplia referencia al principio de proporcionalidad. Sin embargo, nos inclinamos por la primera opción, dado que ello se corresponde con la regulación de esta medida respecto de los delitos contemplados en los artículos 367, 367 ter, 367 quáter, incisos primero y segundo, y 367 septies, según el artículo 369 ter, todos del Código Penal. Es decir, era una medida ya prevista en materia de explotación sexual comercial de niños, niñas y adolescentes en las mismas condiciones que ahora exponemos, a diferencia de lo regulado en materia de la Ley 20.000, en que la medida no exige la autorización judicial.

Sin embargo, y a diferencia de lo acontecido en materia de pornografía infantil, en que la medida no ha resultado de utilidad, dado que la normativa no contiene una exención explícita de responsabilidad por los delitos en los que se pueda incurrir en el desarrollo de la actividad, en materia de delitos informáticos la situación legislativa es distinta. Así, la regulación del Código Penal, en el artículo 369 ter, no contiene una disposición tan clara como la que contempla la parte final del inciso final del artículo 12 de la LDI, según el cual «El agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma».

Los problemas que la disposición puede plantear en términos de la actuación del agente, de forma de excluir la provocación para la comisión del delito, así como otros inconvenientes en la materia, deberían quedar superados por la amplia experiencia que en este ámbito ha proporcionado la investigación del narcotráfico.

Sin embargo, y pese a la ventaja en la regulación de la medida por sobre lo legislado en materia de ESCNNA y la experiencia adquirida en materia de narcotráfico, la herramienta puede presentar problemas

asociados a dos cuestiones prácticas. En primer lugar, en cuanto a las exigencias que los jueces efectúen respecto de los detalles técnicos de la diligencia. Es lógico que desde el rol judicial puedan existir estas solicitudes, pero de materializarse ese conocimiento al interior del proceso, se perdería la posibilidad de recurrir al mismo medio tecnológico en el futuro, medio que, lejos de ser «desechable», puede haber sido sumamente costoso en términos económicos. En segundo lugar, existe un problema respecto de los resguardos para el funcionario policial que actúa como agente encubierto. Recordemos que esta diligencia está asociada, en general, a casos de delincuencia organizada, pero, además, que estamos hablando del «ciberespacio», vale decir, de ausencia de límites, de fronteras; por el contrario, hablamos de lugares donde todas las personas nos encontramos, podemos actuar e interactuar en muchísimos ámbitos, por lo que la inexistencia absoluta de resguardos que eviten la amplia gama de represalias que puedan sufrir los funcionarios y funcionarias es un problema a considerar.[207]

Para solucionar los inconvenientes que una diligencia que puede ser de mucha utilidad en las investigaciones ocasione en la práctica, deberá mirarse la experiencia de otros sistemas que la contemplen y estudiarse cómo han abordado tales inconvenientes. Por ejemplo, podemos citar el caso español, donde la medida se contempla previa autorización judicial para canales de comunicación cerrados y sin autorización para casos urgentes, en que, una vez realizada la diligencia, se deberá poner en conocimiento judicial en un plazo máximo de 24 horas.

C) Tratamiento de los antecedentes de investigación que se encuentren en formato electrónico

El artículo 14 de la LDI se refiere a este punto, y dispone que los antecedentes de investigación que se encuentren en formato electrónico y estén contenidos en documentos electrónicos o sistemas informáticos, o que correspondan a datos informáticos, serán tratados en conformidad a los estándares definidos para su preservación o custodia en el procedimiento respectivo, de acuerdo con las instrucciones generales que al efecto dicte el fiscal nacional.

207 Respecto de estos puntos relativos a la práctica investigativa, se agradece particularmente la información proporcionada por la Brigada Cibercrimen de la PDI, en entrevista sostenida con fecha 21 de febrero de 2024. Sin embargo, en este punto es preciso considerar las mejoras introducidas por la Ley 21.694.

Es bastante lógico que se requiera una normativa reglamentaria que regule la materia, porque no resulta óptimo que la ley, atendida la vertiginosidad y especificidad técnica de los tópicos, sea la encargada de esos menesteres. Pero sí es necesaria alguna regulación, dadas todas las características que presenta este tipo de evidencia, a las que hemos hecho referencia a lo largo de estas páginas: su volatilidad, facilidad de eliminación y modificación, etc. La preservación correcta de la evidencia es fundamental a la luz del respeto a las garantías, particularmente en materia de derecho a defensa. Se precisa, entonces, cierta certeza jurídica que, si no la proporciona la ley, debe hacerlo algún marco normativo.

Coherentemente con un sistema acusatorio, la ley asigna esa labor al órgano encargado de la persecución penal, el que debe tener la capacidad, especialización y flexibilidad necesaria para hacerse cargo del desafío. A la fecha, en todo caso, la Fiscalía no ha dictado la instrucción a la que alude esta norma.

D) Preservación provisoria de datos informáticos

El artículo 218 establece que «[…] el Ministerio Público con ocasión de una investigación penal podrá requerir, a cualquier proveedor de servicio, la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega. Los datos se conservarán durante un período de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días. La empresa requerida estará obligada a prestar su colaboración y guardar secreto del desarrollo de esta diligencia».

Esta norma equivale a lo que el Convenio de Budapest denomina conservación rápida de los datos informáticos almacenados en su artículo 16, con la particularidad de que queda condicionada a una orden judicial que sería inminente o se estaría tramitando para efectos de obtener la entrega de los mismos. En este caso, la disposición no distingue entre datos relativos al tráfico o datos relativos al contenido, por lo que entendemos que ambos están incorporados. Además, en este caso se establece un tiempo de duración, lo que suele ser discutible por los costos que ello pueda implicar para las empresas afectadas.

E) Registro de llamadas y otros antecedentes de tráfico comunicacional

Finalmente, una medida que podemos incorporar dentro de este ámbito dice relación con la contemplada en el artículo 218 ter del CPP.[208] Si

208 Artículo 218 ter. «Registros de llamadas y otros antecedentes de tráfico comunicacional. Cuando existan fundadas sospechas basadas en hechos determinados y ello sea útil para la investigación, el Ministerio Público podrá requerir a cualquier proveedor de servicios, previa autorización judicial, que entregue la información que tenga almacenada relativa al tráfico de llamadas telefónicas, de envíos de correspondencia o de tráfico de datos en Internet de sus abonados, referida al período de tiempo determinado en la resolución judicial.

Para efectos de este artículo se entenderá por datos relativos al tráfico todos aquellos referidos a una comunicación realizada por medio de un sistema informático o de telecomunicaciones, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

El Ministerio Público podrá requerir, en el marco de una investigación penal en curso y sin autorización judicial, a cualquier proveedor de servicios que ofrezca servicios en territorio chileno, que facilite los datos de suscriptor que posea sobre sus abonados, así como también la información referente a las direcciones IP utilizadas por estos para facilitar la identificación de quienes corresponda en el marco de la investigación. Los proveedores de servicios deberán mantener el secreto de esta solicitud.

Por datos de suscriptor se entenderá aquella información que posea un proveedor de servicios relacionada con sus abonados, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, tales como la información del nombre del titular del servicio, número de identificación, domicilio, número de teléfono y correo electrónico. Las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de Internet deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de un año, una nómina y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios.

Los funcionarios públicos, los intervinientes en la investigación penal y los empleados de las empresas mencionadas en este artículo que intervengan en este tipo de requerimientos deberán guardar secreto acerca de ellos, salvo que se les cite a declarar.

La entrega de los antecedentes deberá realizarse en el plazo que disponga la resolución judicial. Si el requerido estima que no puede cumplir con el plazo en atención al volumen y la naturaleza de la información solicitada o la información no existe o no la posee, deberá comunicar dicha circunstancia fundadamente al tribunal, dentro del término señalado en la resolución judicial respectiva.

Si a pesar de las medidas señaladas en este artículo la información no es entregada, podrá ser requerida al representante legal de la institución u organización de que se trate, bajo apercibimiento de arresto.

bien la LDI no hace una referencia explícita a esta norma, la misma es de aplicación general por estar contenida en el código del ramo y, por tanto, ser aplicable a cualquier categoría de delictiva en el caso de encontrarnos ante los supuestos de hecho que la hagan procedente.

Lo particular es que tanto esta disposición como otras a las que aludimos en materia de interceptación de comunicaciones no provienen de la LDI, sino de la Ley 21.577, que fortalece la persecución de los delitos de delincuencia organizada, establece técnicas especiales para su investigación y robustece comiso de ganancias, lo que también es relevante para ratificar que la obtención de evidencia digital es un fenómeno transversal y al que debemos poner mayor atención en ámbitos, precisamente, de mayor complejidad.

El artículo define varios de los conceptos aludidos en el Convenio de Budapest, como datos relativos al tráfico, abonados y suscriptores, y los procedimientos y las obligaciones que adquieren los proveedores de servicios.

La infracción a la mantención de la nómina y registro actualizado de los antecedentes a que se refiere el inciso cuarto será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la Ley N° 18.168, General de Telecomunicaciones. El incumplimiento de las obligaciones de mantener con carácter reservado y adoptar las medidas de seguridad correspondientes de los antecedentes señalados en dicho inciso, será sancionado con la pena prevista en la letra f) del artículo 36 B de la Ley N° 18.168. Los registros así obtenidos quedarán bajo custodia del Ministerio Público, quien cuidará que los datos en cuestión no sean conocidos por terceras personas.

Los registros solo podrán ser utilizados para los efectos de la investigación en la que fueron solicitados, u otras seguidas por delitos que merezcan pena de crimen o sean propias del sistema de análisis criminal y focos investigativos, de acuerdo con lo establecido en el artículo 37 bis de la Ley N° 19.640, que establece la ley orgánica constitucional del Ministerio Público, y no podrán ser utilizados para otros fines.

El ejercicio de esta facultad se regulará mediante instrucciones generales dictadas por el Fiscal Nacional, conforme a lo establecido en el artículo 17 letra a) de la Ley N° 19.640, con el objeto de asegurar su uso racional».

Capítulo 4

Cooperación internacional en materia de ciberdelincuencia

1. Importancia de la cooperación internacional en la persecución penal de la ciberdelincuencia

Como se ha señalado reiteradamente, una de las particularidades importantes en materia de ciberdelincuencia consiste en el hecho de que el entorno cibernético ofrece múltiples oportunidades para los delincuentes en la comisión de delitos, sin atender a límites territoriales, las fronteras de los países o el concepto de soberanía nacional. Los delincuentes se pueden trasladar de una jurisdicción a otra, no solo en términos físicos, sino también informáticos o virtuales, además de los distintos lugares en que se pueden encontrar las víctimas, las evidencias de los actos delictivos, las empresas proveedoras de servicios y, por ende, de información, o en que los efectos de los delitos se pueden producir. Todo ello hace que la cooperación internacional sea primordial.

El Convenio de Budapest no es el único tratado internacional que existe en materia de ciberdelincuencia; también están, por ejemplo, con alguna referencia al punto los Convenios de Lanzarote y Estambul y, particularmente, la Convención de Malabo, que es un acuerdo de la Unión Africana sobre ciberdelincuencia y protección de datos personales que contiene importante regulación sobre transacciones electrónicas, protección de datos personales, ciberseguridad y ciberdelincuencia. Sin embargo, Budapest es el instrumento internacional más importante en lo que dice relación con la cooperación internacional en este tópico, cuestión que viene a reafirmar con su Segundo Protocolo Adicional, justamente referido a una *cooperación reforzada y a la revelación de pruebas electrónicas*.

El Convenio de Budapest incluye varios instrumentos de cooperación internacional, algunos de ellos son comunes a otros tratados internacionales, pero otros son exclusivos de este tratado. A la vez, contiene

disposiciones específicas, por ejemplo, con relación a la conservación rápida de datos, la revelación de datos, la asistencia jurídica mutua en lo que respecta a la obtención en tiempo real de datos relativos al tráfico y de los datos relativos al contenido.

A continuación, revisaremos las normas del Convenio sobre Ciberdelincuencia del Consejo de Europa en materia de cooperación internacional, así como las contenidas en su Segundo Protocolo Adicional, suscrito también por nuestro país.

2. Principios generales relativos a cooperación internacional en el Convenio de Budapest

La regulación comienza con una norma de carácter general que constituye una declaración en cuanto a que las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del Capítulo III, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

3. Extradición

En materia de extradición[209], el Convenio la aplica en su parte sus-

209 Artículo 24: «Extradición
1. El presente artículo se aplicará a la extradición entre las Partes por los delitos definidos de conformidad con los artículos 2 a 11 del presente Convenio, siempre que sean castigados por la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración de al menos un año, o con una pena más grave.
b. Cuando se aplique una pena mínima diferente en virtud de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE N° 24), o de un acuerdo basado en legislación uniforme o recíproca, se aplicará la pena mínima prevista en dicho tratado o acuerdo.
2. Se considerará que los delitos descritos en el párrafo 1 del presente artículo están incluidos entre los delitos que pueden dar lugar a extradición en todos los tratados de extradición concluidos entre o por las Partes. Las Partes se comprometerán a incluir dichos delitos entre los que pueden dar lugar a extradición en todos los tratados de extradición que puedan concluir.
3. Cuando una parte que condicione la extradición a la existencia de un tratado reciba una demanda de extradición de otra Parte con la que no ha concluido ningún tratado de extradición, podrá tomar el presente Convenio como fundamento jurídi-

tantiva, es decir, la regula respecto de los delitos que se contemplan en el Convenio y sobre los que, conforme al texto del mismo, los Estados suscriptores se han obligado a legislar. Adiciona el requisito, para efectos de extradición, de que tales delitos sean castigados por la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración mínima de un año. En todo caso, y como suele ser una regla en el Convenio, ello aplicará salvo que los Estados tengan entre sí otra herramienta internacional que los rija en materia de extradición. Pero, a la vez, agrega que en todos los tratados de extradición que se puedan encontrar concluidos entre los países se debe incorporar los delitos informáticos que contempla el Convenio, en tanto que los Estados también asumen el deber de incorporarlos en aquellos tratados que aún no estén concluidos.

En caso de no existir tratado vigente entre los países, cobra total vigencia el Convenio sobre Ciberdelincuencia del Consejo de Europa, aunque las normas sobre extradición pasan a regirse por el derecho interno de cada país, incluyendo los motivos para negar lugar a la extradición.

---

co de la extradición en relación con cualquiera de los delitos previstos en el párrafo 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el párrafo 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5. La extradición estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de extradición vigentes, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Si se deniega la extradición por un delito mencionado en el párrafo 1 del presente artículo únicamente por razón de la nacionalidad de la persona reclamada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes a efectos de la acción penal pertinente, e informará, a su debido tiempo, de la conclusión del asunto a la Parte requirente. Dichas autoridades tomarán su decisión y realizarán sus investigaciones y procedimientos del mismo modo que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7. a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de las demandas de extradición o de detención provisional, en ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro».

4. Asistencia jurídica mutua

La asistencia jurídica mutua es el procedimiento jurídico por el cual los países se prestan recíproca colaboración y apoyo en las investigaciones penales que están llevando adelante y que, en un mundo globalizado, cobra mayor vigencia y relevancia día a día.

En general, los instrumentos internacionales existentes en la materia regulan la forma en que los estados se prestan colaboración para la obtención e intercambio de evidencia, pero también incluye otras cuestiones como las relativas a la extradición o la regulación de los procedimientos de asistencia mutua, entre los que se incluye las causales para rechazar tal cooperación.

Lo anterior no obsta a que existan mecanismos informales de cooperación entre los órganos aplicadores de la ley en los distintos países, pero es preciso tener presente que lo que se obtenga como resultado de la cooperación informal servirá para desarrollar líneas investigativas, mas no para incorporarse formalmente como prueba al interior de un procedimiento judicial, pues para ello ha debido seguir el camino formal de la asistencia jurídica.

El artículo 25[210] contempla los principios generales aplicables a la asis-

210 Artículo 25: «Principios generales relativos a la asistencia mutua

1. Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.

2. Cada Parte adoptará asimismo las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35.

3. Cada Parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación.

4. Salvo en caso de que se disponga expresamente otra cosa en los artículos del presente Capítulo, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal.

5. Cuando, de conformidad con lo dispuesto en el presente Capítulo, la Parte re-

tencia mutua, pero es importante hacer presente que toda esta normativa aplicará únicamente en ausencia de otros tratados que rijan entre los países, vale decir, el objeto del convenio es servir para la aplicación supletoria y cobertura de lagunas que los Estados suscriptores puedan tener entre sí, sin perjuicio de su aplicación directa en ausencia de normativa.

5. Información espontánea

La primera norma relativa a esta cooperación mutua se refiere a la simple posibilidad de que un Estado comunique a otro la información que haya obtenido en el marco de una investigación penal y que estime que puede ser conveniente que otro Estado la conozca. Esta utilidad puede decir relación con las investigaciones que el otro Estado pueda iniciar o concluir en materia de ciberdelincuencia, o bien la información puede servir para, posteriormente, fundar una solicitud de cooperación internacional hacia el Estado informante.

En todo caso, el Estado informante puede solicitar que la información que transmite sea tratada con reserva o que se utilice solo bajo ciertas condiciones, cuestión que el Estado receptor debe decidir si acepta o no. Si, por el contrario, no se encuentra en condiciones de cumplir con la confidencialidad o restricciones, debe informarlo al país original, el que, sobre la base de ese conocimiento, decidirá si proporciona o no la información de que dispone.

Podemos encontrar un ejemplo de esta medida en las investigaciones desarrolladas en materia de distribución de material pornográfico infantil, en que un país, en el marco de sus propias investigaciones, puede tener conocimiento de direcciones IP asociadas a otros países. Ocurrió en una investigación llevada cabo por el FBI en que este contaba con un agente encubierto. Su agente encubierto tomó contacto con nacionales belgas, con quienes se compartían material audiovisual de abuso infantil. Estados Unidos informó de los hechos a las autoridades belgas, quienes iniciaron una investigación con los datos proporcionados.

---

querida esté autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerará que dicha condición se satisface si el acto que constituye delito, y para el que se solicita la asistencia mutua, está tipificado como tal en su derecho interno, independientemente de que dicho derecho interno incluya o no el delito en la misma categoría o lo denomine o no con la misma terminología que la Parte requirente».

6. Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Como se dijo, el Convenio se aplicará directamente en ausencia de acuerdos internacionales entre las partes. Para tales efectos, cada uno de los países suscriptores deberán designar una o más autoridades centrales, las que serán informadas al secretario general del Consejo de Europa. Sin embargo, en casos urgentes se contempla la posibilidad de que los Estados recurran directamente a las autoridades homólogas, saltándose a la autoridad central. Por ejemplo, de fiscalía a fiscalía cuando no sea esta la autoridad central, sino, por ejemplo, la cancillería.

Cuando existan los requerimientos, estos se ajustarán al derecho del Estado requirente, salvo que se contrapongan a lo establecido por el Estado requerido.

Entre los motivos de denegación que se contemplan están los propios del derecho interno de cada Estado y se considera expresamente que la Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2° a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal. Además, se adicionan las siguientes causales de negativa:

- si la solicitud tiene que ver con un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
- si la Parte requerida estima que acceder a la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

La parte requerida puede, en todo caso, aplazar el cumplimiento de la solicitud cuando estime que su ejecución puede mermar sus propias investigaciones, todo lo cual deberá informar al Estado requerido. También deberá motivar las razones de denegación de la solicitud en caso de que corresponda. Por otro lado, el Estado requirente puede solicitar el tratamiento confidencialidad de la solicitud en caso de requerirlo, cuestión que deberá ponderar el Estado requerido.

7. Disposiciones específicas de asistencia mutua en materia de medidas provisionales

En esta sección se comentará sobre las disposiciones específicas de asistencia mutua en materia de medidas provisionales.

7.1. Conservación rápida de los datos informáticos almacenados y revelación parcial de datos relativos al tráfico

Al igual que lo señalado en la sección procesal de derecho interno del Convenio de Budapest, la conservación rápida se trata de una medida procesal que las autoridades del orden penal pueden adoptar con el fin de evitar la modificación o eliminación de los datos informáticos que ya se encuentren almacenados, de modo que, cuando la orden se dicta, la persona responsable de los datos tiene la obligación de conservarlos. Lo mismo está contemplado en el plano de cooperación internacional, con la única exigencia de que se señale que posteriormente se procederá a una solicitud formal para acceder a los datos mismos o a su registro.

No se trata, según lo ya analizado, de una medida intrusiva, por cuanto la persona o entidad sigue teniendo el control de los datos; de hecho, la autoridad penal ni siquiera accede a ellos, solo se propende a su conservación íntegra.

Se trata de una medida de orden provisional, mientras se obtengan las órdenes judiciales pertinentes, y puede afectar a los datos sin distinción, vale decir, tanto a aquellos relativos al tráfico como a los que apuntan directamente al contenido.

Una vez recibida la orden, la autoridad requerida adoptará todas las medidas necesarias para velar por la conservación de los datos.

Se trata, entonces, de una medida que permite congelar a nivel transfronterizo todo tipo de datos de forma muy rápida y relativamente informal, mientras se obtienen o tramitan las solicitudes formales de asistencia jurídica.

En cuanto a la revelación de los datos informáticos prevista en el artículo 30 del Convenio, cabe destacar que se trata de dar un paso más allá de la conservación y, de algún modo, aunque sea mínimo, obtener acceso a algunos datos. Y esto es relevante porque implica que en muchos países ello puede requerir de autorización judicial para efectos de su

concreción. Por lo anterior, pudiera ser extraño que el Convenio lo trate como una solicitud entre autoridades centrales, pero debemos considerar que se trata siempre de un conjunto muy limitado de datos, relativos únicamente al tráfico, de modo que la garantía básica de la intimidad no se vería conculcada.

7.2. Acceso a los datos informáticos almacenados

El registro y la confiscación son medidas investigativas que todos los sistemas contemplan. La particularidad, en este caso, es que el registro no discurre sobre la base de uno de carácter físico, respecto de cosas tangibles, sino que se refiere a la posibilidad de que las autoridades de un Estado le soliciten a las de otro la realización de un registro a un sistema informático y la confiscación de los datos contenidos en él.[211]

7.3. Acceso transfronterizo a los datos informáticos almacenados

Este caso concierne el acceso directo a la información que se encuentra contenida en un sistema informático ubicado físicamente en otro país, lo cual es una disposición sumamente innovadora del Convenio, que aplicará únicamente para casos de información pública o en situación de contarse con el consentimiento de la persona autorizada jurídicamente para dar acceso a esos datos.

Se considera que los datos son de dominio público cuando se trate de cosas a las que se puede acceder a través de la red mundial sin tener que

211 Artículo 31: «Asistencia mutua en relación con el acceso a datos almacenados
1. Una Parte podrá solicitar a otra Parte el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, incluidos los datos conservados de conformidad con el artículo 29.
2. La Parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con las disposiciones pertinentes del presente Capítulo.
3. La solicitud deberá responderse lo más rápidamente posible en los siguientes casos:
a. cuando existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o de modificación; o
b. cuando los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean una cooperación rápida».

superar las barreras de acceso que hacen que ciertos espacios de Internet sean privados o semiprivados. Si una determinada parte del sitio web no está abierta al público, se entiende que no es del dominio público.

En cuanto al consentimiento de la persona autorizada, este debe ser explícito y exento de cualquier medida que coarte su voluntad o la vicie, como podría ser un engaño o amenaza.

7.4. Obtención en tiempo real de los datos relativos al tráfico

El artículo 33 contempla esta medida con relación a comunicaciones específicas transmitidas en su territorio a través de un sistema informático, respecto de los delitos para los cuales sería posible dicho instrumento procesal en el derecho interno, y la medida sigue el mismo procedimiento que la obtención en tiempo real de los datos relativos al contenido, o interceptación de las telecomunicaciones, a la que nos referimos a continuación.

7.5. Interceptación de las telecomunicaciones

La medida de interceptación de comunicaciones telefónicas está prevista prácticamente en todos los ordenamientos, siempre como una de las de carácter más intrusivo que existen. Sin embargo, la novedad que incorpora el Convenio en este caso es que no se refiere únicamente a las comunicaciones telefónicas, no solo a la voz.

Es importante destacar que, en el caso de las dos últimas medidas, vale decir, de obtención de datos en tiempo real, el Convenio establece la limitación de sujeción al derecho interno, lo cual es particularmente relevante porque se trata de las medidas, como señalamos, más intrusivas que suelen contemplar los ordenamientos, de modo que se consignan las restricciones propias de sus legislaciones en un marco de reciprocidad.

8. La Red 24/7

Como se ha venido sosteniendo reiteradamente, una de las particularidades tanto en materia de delitos informáticos como de la evidencia electrónica que puede recogerse no solo en estos delitos, sino en cualquiera, consiste en su volatilidad; por lo tanto, el sentido de urgencia

cobra un vigor inusitado en la materia. En este sentido, una de las disposiciones más relevantes y útiles que el Convenio de Budapest contempla es el establecimiento de la Red 24/7.

La principal finalidad de esta red de contactos es lograr la materialización urgente de las medidas de cooperación internacional que se requieran, previo a toda la labor de asesoramiento que pueda ser necesaria en un caso específico. La red se concibe especialmente para el éxito de medidas de congelamiento urgentes que se requieran para evitar la pérdida de evidencia.

En general, los puntos de contacto que los Estados partes han fijado constituyen entes policiales o de fiscalía. En el caso chileno, el punto de contacto 24/7 está constituido por la Unidad de Cooperación Internacional y Extradiciones de la Fiscalía Nacional del Ministerio Público (UCIEX).[212]

9. Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas

Si bien el Convenio de Budapest sigue plenamente vigente, actualizado y con la importancia a la que hemos aludido a lo largo de estas páginas, sobra referirse al vertiginoso avance de la tecnología, que exige instrumentos adicionales que puedan hacerse cargo de cuestiones específicas y, sobre todo, en los momentos oportunos. Se trata de afrontar el tremendo desafío de que la regulación vaya a la par del avance tecnológico o, a lo menos, que no quede muy desfasada.

Esta es la razón de ser del Segundo Protocolo Adicional al Convenio, que intenta sortear principalmente el reto de enfrentar de modo adecuado, desde el ámbito penal, las complejidades que representa la obtención de prueba digital en la nube.

En el caso de los datos y las evidencias almacenadas en la nube, el problema no solo dice relación con su ubicación fuera del Estado requirente, sino que muchas veces la complejidad radica en lo difuso de la información relativa a su ubicación geográfica, por lo que ni siquiera se conoce el régimen jurídico al que está sujeta la información o los datos, de modo que las herramientas tradicionales en materia de cooperación internacional también pasan a tener un alcance más limitado.

212 En la actualidad el jefe de dicha unidad es el abogado Juan Pablo Glasinovic, correo electrónico: jpglasinovic@minpublico.cl.

Por lo anterior, existen legislaciones que han permitido a sus autoridades penales el acceso transfronterizo a los datos inclusive de un modo unilateral, pero sin duda lo óptimo sería la existencia de un marco regulatorio que pueda dar certeza jurídica en la materia.

En el año 2016 se desarrolló la Conferencia de Ámsterdam, en la que se exploraron, en el marco de algunas deficiencias detectadas en la evolución y aplicación del Convenio de Budapest, soluciones específicas para el intercambio público-privado de datos y la identificación de situaciones en las que se desconoce la ubicación de los datos o los responsables de su tratamiento. El Convenio sobre Ciberdelincuencia cuenta con un comité que busca, entre otros objetivos, el adecuado seguimiento a las disposiciones del Convenio y su correcta actualización.

En la Conferencia se evidenció la obligación general que tienen los Estados de proteger a la sociedad y a las personas contra la ciberdelincuencia. En vista de ello, se tuvo presente que el acceso a las pruebas ubicadas en la nube (en jurisdicciones extranjeras, desconocidas o múltiples) es cada vez más necesario, a efectos de desarrollar las investigaciones penales regulares. De hecho, existe la idea de que hay una cifra negra importante en materia de ciberdelitos, por cuanto la situación de no saber dónde se cometió el delito, qué aparatos fueron utilizados, quién pudo haber sido el responsable y la poca expectativa de obtener evidencias para acreditarlo desincentivan las denuncias. Se precisa de la cooperación voluntaria por parte de los proveedores de servicios internacionales, especialmente en lo que dice relación con información relativa a los abonados y en situaciones de emergencia, todo lo cual hace necesario un protocolo adicional al Convenio.

El Protocolo cubre los siguientes aspectos:

- Idioma de las solicitudes.
- Solicitudes de información sobre registros y nombre de dominio.
- Revelación directa de los datos relativos al abonado.
- Ejecución de órdenes de otra Parte para acelerar la presentación de datos.
- Solicitudes de información sobre el registro de nombres de dominio.
- Revelación rápida de datos informáticos en caso de emergencia.
- Asistencia jurídica mutua en caso de emergencia.
- Videoconferencias.
- Equipos conjuntos de investigaciones e investigaciones conjuntas.

En resumen, el Protocolo permite a las autoridades de una Parte dirigirse directamente a una entidad proveedora de servicios de otro territorio para pedirle la divulgación de los datos relativos a los abonados, por cuanto se evidenció la necesidad de tratar los datos relativos a los abonados de forma diferente a los datos relativos al tráfico y al contenido, en cuanto a los diferentes procedimientos y mecanismos que deben seguirse para lograr la obtención de cada uno de ellos. La información sobre los abonados es necesaria para conocer al propietario de una cuenta de redes sociales, correo electrónico o un usuario de una dirección de IP.

Además, el Protocolo adopta un sentido de mayor urgencia en ciertas situaciones críticas, de modo que se contemplan dos disposiciones a este respecto: una de ellas permite la divulgación rápida de los datos almacenados (artículo 9°), incluyendo datos relativos al contenido, y la otra se refiere a la asistencia jurídica mutua en casos de emergencia (artículo 10). Todo ello siempre teniendo presente la salvaguardia de los derechos fundamentales, con expresa alusión, en el caso de este protocolo, a la protección de los datos personales (artículo 14).

La información relativa al registro de un nombre de dominio suele ser una de las claves más importantes para iniciar una investigación penal. Esta información constituye un tipo de datos que, en general, proporcionan de modo informal y voluntaria los servicios Whois, por lo que el protocolo proporciona una base jurídica formal a través de un procedimiento de cooperación directa entre las autoridades un Estado y una empresa extranjera. Lo mismo ocurre con relación a la información relativa a los abonados, en cuyo caso se permite acceder solo a los datos almacenados relativos a los abonados en investigaciones penales específicas.

Luego, el protocolo regula procedimientos específicos en materia de situaciones de emergencia, por las que debemos entender aquellas en que exista un riesgo significativo e inminente para la vida o la seguridad de una persona.

En definitiva, el Convenio y su Segundo Protocolo Adicional contemplan herramientas que pueden resultar sumamente útiles para el esclarecimiento de los hechos constitutivos de delitos, pero que, en muchos países, aún no han podido probarse ni existe la experiencia desarrollada a su respecto que nos permita hacer una evaluación de su operatividad. Por tanto, se trata de una materia no solo en constante evolución, sino

a la que urge hacerle el debido seguimiento, que nos permita mantenernos actualizados y anticiparnos a realidades que antes podían parecer lejanas, pero que el ciberespacio las trae a la actualidad.[213]

10. Buenas prácticas de cooperación internacional aceptadas por la jurisprudencia

Además de las convenciones y otros acuerdos entre Estados para promover y regular la cooperación internacional en materia de ciberdelincuencia, existen algunos acuerdos con organizaciones no gubernamentales, destinados a establecer algunas buenas prácticas, las que han tenido interesantes resultados tanto en la prevención como en la sanción de delitos relativos al secuestro y la explotación sexual, económica y comercial de niñas, niños y adolescentes, a través de, o favorecidos por medios informáticos.[214]

Ya hemos mencionados que una de las complejidades en la investigación de los delitos informáticos, ya sea de los específicos o informáticos propiamente tal, así como de aquellos cometidos a través de medios tecnológicos, es que las empresas que prestan los servicios de Internet o las plataformas de redes sociales, como Instagram, Facebook, WhatsApp, etc., tienen sus servidores o domicilios en lugares distintos a aquellos

213 Por ejemplo, respecto de los equipos conjuntos de investigación, hace unos años Segovia (2018), p. 93, sostenía que «Dentro de las herramientas creadas para una más eficaz cooperación internacional destaca la de los equipos conjuntos de investigación, cuya formación presenta innumerables ventajas en contraste a la cooperación tradicional. Sin embargo, y a pesar de sus evidentes beneficios, las experiencias en la región han sido escasas o casi nulas.

Es posible, sin embargo, y atendido el marco normativo internacional y doméstico vigente en nuestro país, constituir equipos conjuntos de investigación en casos concretos, lo cual sin duda permitirá avanzar en mecanismos novedosos que al menos en principio –sin perjuicio de las evaluaciones que se realicen de las primeras experiencias– tendrán un impacto significativo para el avance y conclusión de investigaciones criminales con conexiones internacionales, favoreciendo de este modo un abordaje integral y respetuoso de garantías de todos los intervinientes de aquellos fenómenos criminales que por sus características y dinámicas, son de preocupación de la comunidad internacional en su conjunto y demandan colaboración entre los Estados involucrados».

214 El contenido de este acápite corresponde, en importante medida, a información proporcionada por el director de Unidad Especializada en Delitos Sexuales de la Fiscalía Nacional, abogado Maurizio Sovino, en entrevista realizada con fecha 25 de octubre de 2023.

donde se cometen los delitos. Varias de estas empresas están domiciliadas o prestan servicios en Estados Unidos.

Los proveedores de servicios electrónicos con sede en Estados Unidos o que presten servicios en ese país, de acuerdo con la legislación federal,[215] deben informar los incidentes de «pornografía infantil aparente».[216]

Para cumplir con esta obligación, las empresas prestadoras de servicios de Internet y plataformas de redes sociales establecen cláusulas en el contrato de prestación del servicio que se aceptan como parte de las condiciones de uso, y que establecen que en el evento que el usuario visite páginas, sitios con imágenes o contenido de material de explotación sexual, autoriza a que la empresa prestadora informe al Centro Nacional para Menores Desaparecidos y Explotados (NCMEC, por su sigla en inglés).[217]

Esta organización es una ONG sin fines de lucro, creada en 1983 por los padres de un niño desaparecido y otros defensores de la niñez y financiada en gran parte por el Congreso de EE. UU. Entre sus múltiples actividades, esta entidad administra el CyberTipline del NCMEC, un sistema centralizado en Estados Unidos para denunciar la explotación infantil en línea. Los proveedores de servicios electrónicos y el público en general pueden denunciar las sospechas de engaño en línea de los niños con fines sexuales, abuso sexual infantil extrafamiliar, explotación sexual infantil, turismo sexual infantil, tráfico sexual infantil, envío de materiales pornográficos no solicitados a niños, nombres de dominio engañosos y palabras o imágenes digitales engañosas en Internet. Cada información o indicio se denomina CyberTip.

El personal del NCMEC revisa cada CyberTip (pista informada a la CyberTipline) y trabaja para encontrar una posible ubicación del in-

215 De conformidad con 18 U.S.C. § 2258A(a)(1), un proveedor de servicios electrónicos está obligado a proporcionar un informe de cualquier aparente pornografía infantil a la CyberTipline del NCMEC. Este informe puede incluir información sobre el individuo, la referencia histórica, la ubicación geográfica, etc. Disponible en https://www.govinfo.gov/content/pkg/USCODE-2011-title18/html/USCODE-2011-title18-partI-chap110.htm, y en https://www.missingkids.org/es/ourwork/ncmecdata

216 De acuerdo con nuestra normativa interna, ya no es correcto hablar de «pornografía infantil», sino de explotación sexual y/o material pornográfico o de explotación.

217 National Center For Missing & Exploited Children.

cidente denunciado, a fin de ponerla a disposición de los servicios de policía, Ministerio Público o la judicatura para que eventualmente se inicie una investigación.

La NCMEC ha suscrito diversos convenios con actores y agentes de las fuerzas del orden y la justicia penal en numerosos países del mundo, para alertar cuando usuarios de ese país visiten páginas con imágenes o contenido de material de explotación sexual a NNA. Los convenios definen contrapartes: en Chile lo es el Cibercrimen de la Policía de Investigaciones, en Argentina lo es la Fiscalía de la Nación, etc.

Es importante mencionar que no se informa el contenido de los mensajes, sino la circunstancia de que determinada persona le envió a otra una foto o imagen con contenido que podría ser constitutivo de explotación sexual infantil o adolescente, lo que constituye una *notitia criminis.*

No hay acceso a las conversaciones o mensajes privados, estos hay que pedirlos con autorización judicial. Solamente se envían las fotografías.

Esta alerta es recibida por el Cibercrimen, quien denuncia los hechos a la fiscalía de modo que, una vez iniciada la investigación, a partir de la entrada en vigor de la Ley 21.577, el 15 de junio de 2023, los fiscales pueden solicitar directamente a las empresas que presten servicios de Internet en territorio chileno los datos de suscriptor que posean sobre sus abonados referentes a las direcciones IP utilizadas por estos y otros datos que permitan determinar su identidad, tales como nombre del titular del servicio, número de identificación, domicilio, número de teléfono y correo electrónico.

Antes de la entrada en vigor de esta ley, los fiscales requerían autorización judicial para solicitar esta información.

Junto con solicitar esta información, los fiscales deben pedir a las empresas que preserven la información sobre el contenido de los accesos alertados.

La mayoría de las empresas proveedoras, por ejemplo, Facebook, tienen en sus plataformas la posibilidad de que la policía o las instituciones a cargo de la investigación de los países soliciten esta preservación. Generan cuentas que permiten ingresar a la plataforma y hacer sus solicitudes a los agentes de la ley.

En Chile tiene acceso el Cibercrimen, pero iniciada la investigación, la preservación se solicita a través de la Unidad de Cooperación Internacional y Extradiciones (UCIEX).

Otra forma de colaboración corresponde al ciberpatrullaje que, por ejemplo, realiza el FBI con información reportada en el CyberTipline, ya referido. Consiste en una actividad policial de carácter preventivo, no investigativo. La policía no ingresa a correos o similares, solo monitorea actividades en la red. Por ejemplo, ingresos a un programa *peer-to-peer* (P2P).

Peer-to-peer es un programa computacional que permite compartir información. Quienes ingresan aceptan las condiciones, entre las que está el acceso a los recursos que cada parte ingresa a una «carpeta compartida» (almacenamiento). Si además existe descarga de material pornográfico, se trata de una hipótesis de difusión.

Otras de las funciones del ciberpatrullaje es la formación de una base de datos que, a través de la Interpol, se comparte con policías de todo el mundo y que permite identificar una mayor cantidad de eventuales víctimas. Por ejemplo, un sujeto comparte a través del programa *peer-to-peer* un archivo con miles de imágenes. Tal vez a través de alguna de estas se pueda identificar el lugar donde se encuentra el niño, niña o adolescente que aparece en las imágenes.

Es importante tener presente que en las investigaciones que se inician por reportes de NCMEC la policía tiene los datos de usuario con toda la información registrada en la empresa prestadora del servicio de Internet. En cambio, con los archivos del programa *peer-to-peer*, solo se tiene una IP. En estos casos, se solicita a las empresas información de esa IP. Sin embargo, los servicios de prepagos y la utilización de redes de Internet públicas dificultan estas prácticas investigativas.

En nuestro país, el mayor desarrollo jurisprudencial sobre delitos de violencia sexual contra NNA cometidos en línea se refiere a casos de material pornográfico y en específico a los siguientes aspectos investigativos:

- Ciberpatrullaje policial.
- Comisión de delitos a través de sistemas P2P.
- Reportes NCMEC.

A continuación, haremos referencia a algunos pronunciamientos judiciales en esta materia.

Corte Suprema, rol 3557-09, RUC 0810018402-9, de 18 de agosto de 2009: Actividades policiales realizadas no afectan los derechos de la defensa, dado que no guardan relación con intervenir descargas o comunicaciones. Todos los datos personales de un determinado usuario son obtenidos posteriormente, mediando una orden del Ministerio Público.

Décimo octavo: «[…] el cuestionamiento preciso que se realiza a la actividad desarrollada por la Policía de Investigaciones está circunscrita al mecanismo utilizado y su forma de operar, destinado a obtener preliminarmente su detección como usuario que descargaba material pornográfico infantil. Lo anterior se realizó a través de un mecanismo de identificación del número de los archivos de ese carácter, lo que es considerado por la defensa de […] como una vulneración de la inviolabilidad de sus comunicaciones privadas, ya que no contaron con la necesaria autorización de la autoridad judicial para proceder a ello».

Décimo noveno: «[…] el sistema de programas utilizados por los acusados para 'bajar' la información cuestionada de autos, se realizó en primer lugar a través de la red Internet que es de público acceso, sin establecerse mecanismos privados de comunicación y registro para tales efectos.

Luego, se comunicaron a través de un programa gratuito que existe en la red a disposición de quien lo estime procedente denominado 'Emule' o 'Emule Plus', el que se basa en un sistema de comunicación que consiste en compartir información […] por lo que mal puede hablarse de comunicaciones privadas, operando como un mercado abierto para obtener –en el presente caso– información pornográfica infantil».

Vigésimo: «Que, en cuanto al código 'hash', este en ningún caso […] interviene, registra ni revisa el contenido del material ilícito que está siendo 'bajado' desde la red para su posterior almacenamiento, pues como ya se indicó precedentemente, solo asigna un código a materiales preexistentes respecto de los cuales se sabe fehacientemente que son de contenido pornográfico infantil, y una vez en la red procede a reconocer a otros iguales, sin importar sus diferentes nombres, no siendo necesario revisarlos o abrirlos para saber su contenido».

Juzgado de Garantía de Talca, RUC 2200453621-9, rol O-3432-2022, de 4 de enero de 2023 (ciberpatrullaje): «[…] indagatorias que permitieron establecer que, mediante el uso de plataformas especializadas desarrolladas por 'Federal Bureau of Investigation' (FBI) y del Departamento de Seguridad Nacional de los Estados Unidos de Norteamérica (Homeland Security), se detectó la descarga y distribución de archivos digitales de abuso sexual infantil, a través de las redes P2P, tales como

Ares, Emule, Edonkey, Bittorrent, etc. Las citadas plataformas mantienen una base de datos de archivos de imágenes y videos previamente incautados por dicho cuerpo policial, los que corresponden a material explícito de abuso sexual infantil, archivos a los que previamente se les extrajo su código hash (código alfanumérico único que individualiza cada archivo digital), así el software especializado de forma automatizada detecta a los usuarios que se encuentra difundiendo y, por consiguiente, que mantienen almacenados a disposición de otros usuarios para su descarga. Cabe hacer presente, que cada usuario requiere descargar e instalar un programa que le permita gestionar solicitudes e intercambiar archivos, quedando estas solicitudes (archivos multimedia) disponibles para su descarga, completándose la descarga efectiva del archivo cuando su porcentaje de vaciado corresponde a un 100 por ciento».

5° Tribunal de Juicio Oral en lo Penal de Santiago, RIT 161-2021, RUC 1900244362-K, de 29 de marzo de 2023, sobre reportes NCMEC señala en el considerando cuarto: «Con esta prueba valorada y analizada por el Tribunal conforme a principios de lógica, máximas de experiencia y conocimientos científicamente afianzados permiten establecer de manera, probablemente cierta y más allá de toda duda razonable, la ocurrencia del hecho establecido al comienzo de este considerando, pues los funcionarios policiales Arriagada y Balloqui dieron cuenta de una denuncia por parte de la ONG NCMEC quien a su vez recibió información de la red social Facebook, que daba cuenta que un usuario usando diversos perfiles requería a menores de edad bajo amenazas imágenes o videos con acciones sexuales explícitas y también enviaba imágenes de pornografía infantil a la red».

> Y respecto de la valoración de los reportes CyberTip, en el mismo considerando cuarto se indica: «El documento presentado, no obstante no tener una traducción oficial fue incorporado mediante una explicación detallada por el testigo Arriagada, lo que permitió comprender su contenido y datos de manera que el mismo documento corroboró los dichos del testigo y también de la Comisaría Balloqui y permitió acreditar que el acusado mantenía distintos perfiles en la red social de Facebook, que solicitaba pornografía infantil a terceros y también el informe permitió su individualización completa, *de manera que se le da pleno valor probatorio al documento referido*.
>
> […] No obstante ser un documento en idioma extranjero, el

contenido del mismo fue detallado por los testigos Balloqui y Arriagada, quienes dieron cuenta de la información contenida en el mismo, *ya sea en su soporte documental como digital, siendo sustancial para establecer uno de los hechos de difusión de pornografía infantil*, dándole pleno valor probatorio al mismo» (énfasis añadido).

Respecto de una eventual vulneración de derechos de la defensa, se afirma: «[…] *no se aprecia en esas actividades ninguna vulneración* a las garantías alegadas por la defensa por cuanto *su representado aceptó expresamente las condiciones* de uso de la red social, de otra manera no podría haber dado apertura a las cinco cuentas que mantenía en dicha plataforma y, por tanto, al contravenir el acuerdo con la red social, ésta hizo uso de los derechos que la asisten, sin vulnerar ninguna garantía» (énfasis añadido).

4° Tribunal de Juicio Oral en lo Penal de Santiago, RIT 149-2022, RUC 2001030068-2, de 21 de julio de 2022. Expone en su considerando décimo: «*[…] el tribunal fue eficazmente interiorizado respecto de la naturaleza, estructura y contenido de la información recabada, pues ambos policías fueron claros y precisos en que, si bien la información viene en inglés, no necesitan tener un conocimiento acabado de dicho el idioma*, dado que consisten en informes o consolidados técnicos denominados *CyberTipline, que contienen incidentes relacionados con explotación sexual que diversas plataformas como Google, Instagram, TikTok o Facebook reportan a la plataforma de la ONG y para cuya revisión fueron especialmente capacitados por la ONG NCMEC a principios del año 2020*, de tal modo que para sus análisis no requieren ser informáticos y solo en caso [de] duda se consulta al equipo informático de la misma unidad» (énfasis añadido).

Tribunal de Juicio Oral en lo Penal de Valparaíso, RIT 0-338-2023, RUC 22100120191-7, de 25 de octubre de 2023. En el considerando vigésimo tercero, numeral 4, se afirma: «*[…] fue el propio acusado […], quien al crear una cuenta o nube virtual con la empresa de servicios de Internet Google y su correo Gmail, aceptó las condiciones para la creación de esa cuenta y correo que al modo de un contrato de adhesión se establecen por las empresas proveedoras de servicios de Internet como lo es Google respecto de quienes quieran hacer uso de ellos. De no haber aceptado esas condiciones, como indicó el inspector Garrido Pavés, no podría haber creado el acusado la cuenta ni el correo electrónico.*

[…] *Tampoco vemos en la situación expuesta*, como sugiere igualmente la defensa, un *atentado en contra de nuestra soberanía estatal*, si se considera que el acusado, actuando en base a su autonomía de la voluntad –uno de los principios fundamentales de la legislación contractual civil en Chile– aceptó condiciones como las antes expuestas, permitiendo a Google, como dijo el inspector Garrido Pavés, actuar como moderador respecto del acceso y visualización del contenido de su nube o correo electrónico para verificar la existencia o no de archivos que den cuenta o puedan importar delitos como los ya señalados en contra de menores de edad, renunciando así a una protección normativa dentro de un ámbito que es posible dicha renuncia en base al artículo 12 del Código Civil […].

[…] nada puede levantarse en el caso de marras en contra de la actuación de nuestra policía civil y estimarla ilegal, desde el momento que en virtud de convenios existentes, a través de Interpol, y con capacitación previa de funcionarios de PDI, la policía accedió al reporte de los archivos de pornografía infantil que NCMEC subió a su respectiva plataforma y que le fueron remitidos por Google, en base a las condiciones que se aceptan por los usuarios de sus servicios, correspondientes a la nube virtual del acusado […]».

Referencias

Acuario, Santiago (2016). *Delitos informáticos. Generalidades*. s.l.: Universidad Nacional de Ingeniería.

Aranda, Francisco (2020): «Desafíos de las nuevas tecnologías de la información y de las comunicaciones para el derecho: un paralelismo histórico». *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, (55): 37-63. Valparaíso. Disponible en http://dx.doi.org/10.4067/S0718-68512020000200037.

Arenas, Xabier (2022). «La colaboración eficaz como técnica de investigación en el marco de la Ley de Delitos Informáticos». Memoria para optar al grado de licenciado en Ciencias Jurídicas, Pontificia Universidad Católica de Valparaíso.

Azzolini, Horacio y Nicolás Bru (2017). «Una aproximación a la evidencia digital: tratamiento, adquisición y preservación». En Juan Pérez (coordinador), *Delitos informáticos, investigación criminal, marco legal y peritaje* (pp. 19-39). Buenos Aires: B de F.

Bascur, Gonzalo y Rodrigo Peña (2022). «Los delitos informáticos en Chile: Tipos delictivos, sanciones y reglas procesales de la Ley 21.459. Primera parte». *Revista de Estudios de la Justicia*, (37): 1-38.

BCN (2022). *Historia de la Ley N° 21.459*. Disponible en https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8270/.

BCN (2023). *Historia de la Ley N° 21.595*. Disponible en https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/8195/.

Becker, Sebastián y Pablo Viollier (2020). «La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la ley N° 19.223». *Revista de Derecho*, 88 (248): Pp 75-112.

Borges, Raquel (2018). «La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea». *Revista Boliviana de Derecho*, 25: 536-549.

Bosch, Camila (2018). «Evidencia digital. El Convenio de Budapest y sus desafíos en el derecho procesal penal». *Revista Jurídica del Ministerio Público*, (72): 124-141.

Cárdenas, Claudia (2008). «El lugar de comisión de los denominados ciberdelitos». *Política Criminal*, A2-6: 1-14. Disponible en https://repositorio.uchile.cl/bitstream/handle/2250/126580/Ellugardecomisiondelosdenominadosciberdelitos.pdf;sequence=1.

Carnelutti, Francesco (2000). *La prueba civil*. 2ª edición. Buenos Aires: Depalma.

CNN Chile (2023). «Tras ciberataque: grandes clientes de GTD denuncian 'incalculables daños'». *CNN Chile*, 14 de noviembre. Disponible en https://www.cnnchile.com/pais/ciberataque-gtd-servicio-digital_20231114/.

Cortés, José Luis (2017). «Sobre la distinción de aspectos criminológicos y dogmáticos en el ámbito de la criminalidad informática». *Revista Jurídica del Ministerio Público*, 69: PP- 175-190.

CSIRT (s.f.). «Nuestra misión». Disponible en https://csirt.gob.cl/quienes-somos/nuestra-mision/.

Delgado, Joaquín (2013). «La prueba electrónica en el proceso penal». Diario La Ley, 8167. Disponible en http://diariolaley.laley.es/home/DT0000245602/20170411/La-prueba-digitalConcepto-clases-y-aportacion-al-proceso.

Devis, Hernando (2002). *Teoría general de la prueba judicial*. Bogotá: Temis.

El País (2011). «Yahoo! puede negarse a colaborar con la Justicia belga». *El País*, 12 de octubre. Disponible en https://elpais.com/tecnologia/2011/10/12/actualidad/1318410067_850215.html.

Elmundo.es (2009). «Un tribunal condena a Yahoo! por no colaborar en una investigación», Elmundo.es, 3 de marzo. Disponible en https://www.elmundo.es/elmundo/2009/03/03/navegante/1236069156.html.

Espacios de México (s.f.). «El *phishing* y el *pharming*». Disponible en https://www.espacios.net.mx/que-es-phishing-pharming/.

Etcheberry, Alfredo (2010). *Derecho penal. Parte general, Tomo I*. 3ª edición. Santiago: Editorial Jurídica de Chile.

Fernández, Javier (2007). «Respuesta penal frente a fraudes cometidos en internet: estafa, estafa informática y los nudos de la red». *Revista de Derecho Penal y Criminología*, 2ª época, (19): 217-243.

Faraldo, Patricia (2007). «Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática». *Eguzkilore*. 21:33-57.

Galán, Alfonso (2009): «La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales». *Revista Penal*, (24): https://rabida.uhu.es/dspace/handle/10272/11844

Garrido, Mario (2016). *Derecho Penal Parte Especial, Tomo III, 4ª ed.* Santiago: Editorial Jurídica de Chile.

González, José Miguel (2021). «La prueba pericial digital y la cadena de custodia». *Anales de la Facultad de Derecho*, (38): 43-79. Disponible en https://doi.org/10.25145/j.anfade.2021.38.03.

Horvitz, María Inés y Julián López (2003). *Derecho procesal penal chileno*. Santiago: Editorial Jurídica de Chile.

La Vanguardia (2009). «Un tribunal belga cita a Yahoo! por no colaborar en un caso de delito informático». *La Vanguardia*, 24 de enero. Disponible en https://www.lavanguardia.com/internet/20090124/53625605217/un-tribunal-belga-cita-a-yahoo-por-no-colaborar-en-un-caso-de-delito-informatico.html.

Luque, Sixto, Marcos Salt, Carlos Pinho y Pedro Verdelho (2022). *La prueba electrónica en el marco nacional e internacional en Latinoamérica*. Madrid: Ediciones EL PAcCto. Disponible en https://elpaccto.eu/wp-content/uploads/2022/08/Publicacion-prueba-electronica-EL-PAcCTO.pdf.

Mayer Lux, Laura y Oliver Calderón, Guillermo (2020). "El delito de fraude informático: concepto y delimitación". *Revista Chilena de Derecho y Tecnología*, 9 (1): 151-184.

Mayer, Laura (2017). «El bien jurídico protegido en los delitos informáticos». *Revista Chilena de Derecho*, 44 (1): 235-260. Disponible en http://dx.doi.org/10.4067/S0718-34372017000100011.

Mayer, Laura y Jaime Vera (2022a). «La falsificación informática: ¿Un delito necesario?». *Revista Chilena de Derecho y Tecnología*, 11 (1): 151-184.

Mayer, Laura y Jaime Vera (2022b). «La nueva Ley de Delitos Informáticos». *Revista de Ciencias Penales*, 6ª época, XLVIII (3): 267-336.

Oficina de las Naciones Unidas contra la Droga y el Delito (2022). *Ciberdelito, vol. 1. Guía práctica para un abordaje integral del fenómeno.* https://cdn.www.gob.pe/uploads/document/file/2941907/CYBERDELITO%20VOL%20%2017x24_compressed.pdf.pdf.

ONG Amaranta, ONU Mujeres Chile y Fundación Datos Protegidos (2020). Violencia digital: experiencias virtuales de niñas y adolescentes en Chile. Disponible en https://amarantas.org/ninez-juventudes-e-internet/.

ONU Mujeres (2022). *Informe. Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará*. Disponible en https://lac.unwomen.org/es/digital-library/publications/2022/04/ciberviolencia-y-ciberacoso-contra-las-mujeres-y-ninas-en-el-marco-de-la-convencion-belem-do-para#view.

Oxman, Nicolás (2013). «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, 2° semestre: 211-262.

Regali, Victoria (2021). «Las garantías procesales en la obtención de evidencia digital». *Microjuris*. Disponible en https://aldiaargentina.microjuris.com/2021/04/27/doctrina-las-garantias-procesales-en-la-obtencion-de-evidencia-digital/.

Rodríguez, Luis (2022). *Delitos sexuales. 3ª ed.* Valparaíso: Editorial Jurídica de Chile.

Rodríguez, Marta (2017/2018). «La prueba digital en el proceso penal». Trabajo de fin de máster en Abogacía, Universidad de La Laguna. Disponible en https://riull.ull.es/xmlui/handle/915/7290.

Sain, Gustavo (2017). *Internet, el cibercrimen y la investigación criminal de delitos informáticos. Delitos informáticos, investigación criminal, marco legal y peritaje.* Buenos Aires: B de F.

Sánchez, José (2016). «Estudio de la prueba electrónica en el proceso penal: especial referencia a las conversaciones de WhatsApp». Trabajo de fin de máster en Abogacía, Universidad de Salamanca. Disponible en https://gredos.usal.es/bitstream/handle/10366/132621/TFM_SanchezHernandez_Estudio.pdf?sequence=1.

Segovia, Antonio (2018). «Los equipos conjuntos de investigación como herramienta de cooperación internacional». *Revista Jurídica del Ministerio Público*, 72: 69-98.

Silva, Hernán (2011). «La cooperación eficaz de ley de drogas». *Revista de Derecho y Ciencias Penales*, (17): 211-223.Taruffo, Michele (2008). *La prueba. Artículos y conferencias*. Santiago: Metropolitana.

Troncoso, J. (2023). «Ciberataque a GTD impactó a unas 3.500 corporaciones y del orden de 300 aún se mantienen afectadas». *Diario Financiero*, 2 de noviembre. Disponible en https://www.df.cl/empresas/industria/ciberataque-a-gtd-impacto-a-unas-3-500-corporaciones-y-del-orden-de-300.

Velasco, Eloy (2011). «ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal». *La Ley Penal*, 82: 2-31.

Vera, Alejandro (1996). *Delito e informática (la informática como fuente de delito)*. Santiago: La Ley.

Criminalidad informática y ciberdelincuencia
de Marta Herrera Seguel y Ymay Ortiz Pulgar

Academia Judicial de Chile
Colección Materiales Docentes

DER Ediciones


ACADEMIA
JUDICIAL
CHILE