REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

VOL. 9 NÚM. 2 (2020) • PÁGS. 221-256 • DOI 10.5354/0719-2584.2020.59236
RECIBIDO: 25/10/2020 • APROBADO: 18/12/2020 • PUBLICADO: 31/12/2020

DOCTRINA

El delito de espionaje informático: Concepto y delimitación

The crime of cyber espionage: Definition and delimitation

Laura Mayer Lux y Jaime Vera Vega
Pontificia Universidad Católica de Valparaíso, Chile

RESUMEN El artículo analiza el delito de espionaje informático, con énfasis en su concepto y delimitación. Con dicha finalidad, parte examinando brevemente su injusto en relación con los demás delitos informáticos *stricto sensu*. Luego, estudia su sentido y alcance, su vínculo con otras figuras delictivas y algunos problemas que enfrenta su castigo punitivo. Por último, plantea sugerencias para su futura reforma legal, considerando lo que establece el Convenio sobre Ciberdelincuencia del Consejo de Europa.

PALABRAS CLAVE Cibercrimen, *hacking*, acceso indebido, sabotaje informático, fraude informático.

ABSTRACT This article analyses the crime of cyber espionage, with an emphasis on its definition and delimitation. For this purpose, it starts by briefly examining its unlawful character in regards to other cybercrimes stricto sensu. Subsequently, it addresses its meaning and scope, its relationship with other crimes and some problems facing its punishment. Finally, it also makes suggestions for its future legal reform considering what is established in the Convention on Cybercrime of the Council of Europe.

KEYWORDS Cybercrime, hacking, illegal access, cyber sabotage, cyber fraud.

Planteamiento del problema

El delito de espionaje informático genera una serie de dificultades interpretativas y de delimitación de su injusto. Ellas se hacen más patentes si se considera que el análisis dogmático de la delincuencia informática es aún incipiente[1] y que el espionaje informático ha tenido un escaso tratamiento doctrinal,[2] si se lo compara con otras figuras que integran este sector de la criminalidad, en especial con el fraude informático.[3]

En primer lugar, el sentido y alcance de aquello que denominamos «espionaje informático» no es evidente. En efecto, bajo dicho rótulo suelen incluirse conductas bastante disímiles en su forma de ejecución y gravedad, las que pueden abarcar el mero acceso indebido a datos o programas; pasando por el acceso indebido a sistemas informáticos que importa conocer, de alguna manera, la información en ellos contenida; hasta llegar al acceso a y obtención indebida de datos o programas. Al mismo tiempo, según la clase de información a la que indebidamente se acceda —y que en su caso se obtenga—, será también el bien jurídico afectado por el comportamiento (por ejemplo, el patrimonio, la intimidad, etcétera). Las dos variables apuntadas —forma de ejecución y gravedad, por un lado, bien jurídico, por el otro— suelen estar cruzadas por una tercera variable, a saber, el hecho de que la conducta se lleve a cabo en el ciberespacio, con todas las consecuencias criminológicas y jurídicas que ello conlleva.

En segundo lugar, tampoco es claro cómo castigar el espionaje informático de acuerdo con el derecho penal vigente en todos los supuestos que pueden calificarse de tales. Dicha falta de claridad se vincula con las variables apuntadas *supra*. Así, ya que no todos los casos constitutivos de espionaje informático se ejecutan de igual forma ni tienen idéntica gravedad, pueden surgir dudas al momento de aplicar una misma hipótesis legal a casos que efectivamente son disímiles. Si se considera, además, el bien jurídico subyacente al espionaje informático, es posible que a las normas de la Ley 19.223 se superpongan otras de penalidad no necesariamente equivalente, como los delitos contra la intimidad o privacidad regulados en el Código Penal. En fin, la ejecución en el ciberespacio también puede plantear dificultades, sobre todo si se tiene en cuenta que, por ejemplo, la capacidad de concretar un número indeterminado de comportamientos y de dañar en términos relevantes a terceros muchas veces se ve potenciada por ese especial «contexto» de comisión.

En tercer lugar, no debe perderse de vista que vivimos en una «sociedad de la información», caracterizada por la disponibilidad y el intercambio constante de da-

1. En ese sentido, muchos de los estudios que la abordan tienen un carácter criminológico o político criminal, entre los que destacan Gillespie (2016) y Miró (2012). Respecto de los trabajos de corte más dogmático puede citarse, por ejemplo, a Gercke y Brunst (2009) y Huerta y Líbano (1996).

2. Como excepción a ello, es posible mencionar a Masís (2016) y especialmente a Medina (2014).

3. Que incluso en Chile ha tenido un desarrollo digno de señalar. Véase, por ejemplo, Balmaceda (2009) y Oxman (2013).

tos entre los individuos a través del uso de tecnologías. Dicha circunstancia puede provocar dificultades cuando se busca sancionar (penalmente) el acceso a tales datos, o sea, a informaciones contenidas en un sistema de tratamiento automatizado de las mismas. Lo señalado no sólo plantea desafíos en cuanto a la necesidad de identificar de manera adecuada el injusto del comportamiento a castigar, sino también respecto de qué vamos a exigir de una persona, que es titular de información o está a cargo de ella, para salvaguardar esa información del acceso indebido de otros. Sobre este punto surgen dos visiones, que pueden complementarse con otras intermedias: la que entiende que sólo ha de protegerse penalmente a quien estableció alguna clase de barrera técnica para acceder a la información y la que estima que la tutela penal debe orientarse a todos quienes no consienten en que ella sea objeto de intromisiones.

Considerando los problemas indicados, el presente trabajo aborda el delito de espionaje informático, con énfasis en su concepto y delimitación. Para ello, comienza analizando su injusto en relación con los demás delitos informáticos *stricto sensu*. Más tarde, examina su sentido y alcance, su nexo con otros ilícitos penales y algunos problemas que enfrenta su castigo. Por último, plantea sugerencias para su futura reforma legal, teniendo en cuenta lo que establece el Convenio sobre Ciberdelincuencia del Consejo de Europa (CCCE), del 23 de noviembre de 2001 (del que Chile pasó a ser parte el 28 de agosto de 2017).

Aproximación al injusto de los delitos informáticos[4]

Si se examina el sistema de los delitos informáticos *stricto sensu*, o sea, de las conductas que afectan el software o soporte lógico de un sistema informático (Jijena, 1994: 364; Moscoso, 2014: 13), se advertirá que aquél está integrado, fundamentalmente, por tres figuras delictivas: el sabotaje, el espionaje y el fraude informático (Mayer, 2018: 160 y ss.). Si bien todos esos ilícitos pueden cometerse sin recurrir a internet, los que más importancia práctica tienen son, justamente, ejecutados en el ciberespacio (Miró, 2012: 49).

Sin perjuicio de las precisiones que se efectuarán, a los delitos informáticos en sentido estricto subyacen diversos bienes jurídicos (Magliona, 2002: 384), lo que a su turno depende de la clase de información con la cual se vinculen.[5] Así, por ejemplo, el sabotaje informático puede incidir negativamente en la propiedad si se destruyen o inutilizan datos que tienen un valor económico;[6] mientras que el espionaje informático puede lesionar la seguridad nacional, o bien, la intimidad, si los archivos a los

4. Un examen análogo a éste puede verse en Mayer y Oliver (2020: 154-155).

5. Cuestión diversa es afirmar que el bien jurídico sea la información. Así, en cambio, López (2002: 404-405).

6. En esa línea, Romeo (1988: 175); véase igualmente Corcoy (2007: 18-19).

que se accede —de manera indebida— contienen informaciones secretas de carácter militar o imágenes íntimas de un particular, respectivamente.[7] En fin, el fraude informático, de acuerdo con la tradición europea continental, tiene una clara connotación patrimonial[8] y un medio de comisión específico, a saber, la alteración o manipulación de datos o programas de sistemas informáticos.[9]

Cuando los delitos informáticos *stricto sensu* son perpetrados a través de internet, ellos afectan, además, un bien jurídico común, denominado «funcionalidad informática», esto es, «aquel conjunto de condiciones que posibilitan que los sistemas informáticos realicen adecuadamente las operaciones de almacenamiento, tratamiento y transferencia de datos, dentro de un marco tolerable de riesgo» (Mayer, 2017: 255). Tales condiciones pueden verse afectadas en la interacción que se verifica en el ciberespacio, en términos análogos a lo que ocurre en el tráfico vehicular.[10] En tal evento, delitos como el sabotaje, el espionaje y el fraude informático tendrán un carácter pluriofensivo,[11] puesto que su ejecución vulnerará tanto los intereses vinculados con los datos (intimidad, propiedad o patrimonio, seguridad nacional, etcétera) como la funcionalidad informática, en los términos señalados.

Sentido y alcance del espionaje informático: Relación entre dicho delito y otros ilícitos de la parte especial

El concepto de espionaje no es unívoco y se vincula con distintos comportamientos. Así, de acuerdo con su sentido natural y obvio, que puede consultarse en el *Diccionario de la lengua española*, *espiar* implica, en una dimensión amplia, «acechar, observar disimuladamente a alguien o algo»; mientras que, en una acepción más específica, *espiar* supone «intentar conseguir informaciones secretas sobre un país o una empresa».

En cambio, la noción de espionaje en un sentido jurídico penal encuentra sus principales raíces en el delito del mismo nombre, figura atentatoria de la seguridad del Estado, que se regula en el artículo 109 del Código Penal y en los artículos 252 y ss.

7. Enfatizando en la protección de la privacidad, Medina (2014: 81).

8. Tanto así, que se le concibe como una figura paralela, aunque de naturaleza distinta (Kindhäuser, 1999: 285 y ss.) al tipo de estafa.

9. Por todos, Hilgendorf y Valerius (2012: 148, 157).

10. Dicha analogía nace a partir de la caracterización de internet como una «autopista de la información» (Escalona, 2004: 163), en la que interactúan innumerables individuos. Más en detalle, Mayer (2017: 249).

11. A favor del sentido pluriofensivo de los delitos informáticos *stricto sensu*, si bien con matices respecto de los intereses afectados, Magliona (2002: 384) y Magliona y López (1999: 204-205). En cambio, contrario a su carácter pluriofensivo, Oxman (2013: 225 y ss.).

del Código de Justicia Militar.[12] Se trata de una conducta relacionada con el concepto de «violación de secretos», que puede expresarse ya sea mediante la introducción indebida en la esfera del secreto (intromisión), o bien, a través de la difusión indebida del secreto al que se ha tenido acceso legítimamente (revelación) (Etcheberry, 2010b: 107). Dicho de otro modo, el secreto resulta transgredido, sea porque el propio agente toma conocimiento de la información de que se trate, sea porque la da a conocer a terceros (Acosta, 1988: 70). La idea de *secreto*, a su turno, es definida como «algo conocido por pocas personas que, conforme al interés público o privado, no debe ser publicado o dado a conocer a un círculo más amplio» (Muñoz Conde, 2015: 862).[13] Según veremos, el objeto del secreto puede ser muy variado y dependerá de la clase de informaciones a las que se refiere el mismo (militares, industriales, financieras, profesionales, etcétera).

En una primera aproximación, el término *espionaje informático* también se vincula con la violación de un secreto (en esa línea, Oxman, 2013: 232),[14] caracterizado por estar contenido en un sistema de tratamiento automatizado de la información (Huerta y Líbano, 1996: 296-297).

Espionaje informático, *hacking* y acceso ilícito

El concepto de espionaje informático suele relacionarse con el de *hacking*. Este último, sin embargo, es empleado en diversos sentidos. En términos laxos, la noción de *hacking* es utilizada de manera poco precisa, prácticamente como sinónimo de ciberdelito (Kochheim, 2015: 601). Más específicamente, el *hacking* se identifica con el acceso indebido a (datos de) sistemas informáticos (Sieber, 2014: 437; similar Escalona, 2004: 149; Holt, 2020: 727). Tal definición, en tanto exige un acceso «indebido», comúnmente se vincula con la intención de dañar a otros, supuesto que también se conoce como *cracking* (Moscoso, 2014: 33). Frente a dicha hipótesis, algunos autores aluden a comportamientos —en principio— no lesivos, también denominados *hacking* puro o blanco (Galán, 2009: 94),[15] que involucrarían un mero acceso a datos

12. Véase Balmaceda (2014: 583). Analiza el espionaje como delito contra el derecho internacional Rodríguez (1956: 792).

13. Por su parte, plantea una definición de secreto de corte subjetivo y, por ello, menos idónea para interpretar la relevancia penal del comportamiento, Stern (2007: 188): «[Secreto es] todo aquello que haya querido ser excluido por su titular del conocimiento de terceros».

14. Con todo, el secreto apunta a una característica de la información y no debe confundirse con el bien jurídico.

15. En cambio, desde un punto de vista criminológico, Sestieri (2019: 3-4) diferencia tres categorías de *hacker*: el *black hat*, que permanentemente realiza conductas ilegales; el *gray hat*, que sólo de manera ocasional las lleva a cabo; y el *white hat*, que colabora con la policía, por lo general para identificar fallas de seguridad.

o programas de sistemas informáticos (Oxman, 2013: 234-235). En la misma línea, se dice que el «acceso abusivo a un sistema informático» puede llevarse a cabo con diferentes finalidades: desde averiguar su nivel de seguridad hasta cometer (graves) delitos (Salvadori, 2012: 165-166).[16]

No obstante, tales distinciones han perdido fuerza tanto a nivel doctrinal como normativo. Efectivamente, con el tiempo se ha ido imponiendo la idea de que «la intromisión en sistemas ajenos no tiene cabida, cuanto menos en el marco de la legalidad» y de que «todo *hacking* es *cracking*» (Miró, 2012: 56; similar, Jijena, 1992: 113). Ello también habría[17] sido recogido en el CCCE, que dispone la tipificación del «acceso deliberado e ilegítimo a todo o parte de un sistema informático» (artículo 2, sobre «acceso ilícito»). El mismo precepto que lo regula permite que las partes del Convenio exijan, al tipificar el delito, que éste haya sido cometido «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». Pues bien, en tanto se trata de una facultad del Estado parte, podría no exigirse lo que establece dicha cláusula, con lo que el tipo quedaría circunscrito al mero acceso ilícito a datos o programas.

En el plano terminológico, a pesar de que el CCCE alude a acceso ilegítimo o ilícito, la expresión *espionaje informático* resulta preferible a aquéllas, en especial si consideramos el objeto sobre el que recae la conducta. En ese sentido, el comportamiento que aquí interesa involucra tanto un acceso a los datos como un conocimiento de ellos (en ambos casos, indebido). De forma análoga, la noción de espionaje informático implica que ha habido una intromisión respecto de datos que no deben ser revelados, ya que existen intereses públicos o privados contrarios a que ellos sean conocidos. Por tanto, el sólo acceso ilícito o indebido se solaparía con una etapa de ejecución imperfecta (tentativa) de un auténtico espionaje informático.[18]

En fin, el término *hacking* resulta todavía más inapropiado para dar cuenta de la conducta recién descrita, pues, o se le interpreta como sinónimo de acceso ilegítimo o ilícito —en cuyo caso nos remitimos a lo dicho—, o se le entiende como sinónimo de ciberdelito, posibilidad que impide avanzar en una delimitación adecuada de la intromisión relativa a datos o programas de sistemas informáticos.

16. Véase, asimismo, Gutiérrez (1996: 1163 y ss.). Un análisis histórico del *hacking*, en el que se distinguen cuatro etapas de desarrollo, puede verse en Jordan (2016: 528 y ss.).

17. Decimos «habría», pues la referencia que el CCCE efectúa al acceso ilícito puede interpretarse como mero acceso o como acceso que implica conocimiento de datos. Del mismo modo, la exigencia de ilicitud del acceso puede entenderse como alusiva al conocimiento de los datos o a la vulneración de barreras técnicas.

18. Desde una perspectiva criminológica, Wells (2020: 360) destaca que quienes se introducen (en forma indebida) en sistemas computacionales (ajenos), por lo general no lo hacen por el sólo hecho de acceder a ellos, sino para obtener, revisar, alterar o transmitir datos contenidos en tales sistemas.

Espionaje informático, obtención y revelación de datos

Si el espionaje informático supone tanto acceder a como conocer (indebidamente) los datos contenidos en un sistema informático, su obtención implicaría, en principio, una conducta ulterior y diferenciada del solo acceso y conocimiento. Según su sentido natural y obvio (véase el del *Diccionario de la lengua española*), *obtener* es «alcanzar, conseguir y lograr algo que se merece, solicita o pretende» o «tener, conservar y mantener» una cosa. En esa línea, si bien podría estimarse que quien conoce los datos en algún sentido los obtiene, los casos relevantes de obtención son aquellos que implican almacenar e incluso transferir datos de un sistema informático a otro. Por ende, respecto del espionaje informático, la obtención de datos sería un caso de agotamiento del delito.

Sin embargo, podrían plantearse dudas en supuestos en los que el espía accede y obtiene (en forma indebida) datos, sin conocerlos, por ejemplo, porque los almacena en un *pendrive* o en una nube para que sea un tercero quien pueda conocerlos. Estimamos que en dicha hipótesis cabría aplicar las reglas de la coautoría, en la medida en que haya habido un reparto en la ejecución del tipo penal: o sea, que uno de los sujetos haya accedido a los datos —además de obtenerlos— y otro los haya conocido después.

La idea de revelación o difusión (indebida) de los datos supone incluso algo más que su simple obtención. De acuerdo con su sentido natural y obvio, *revelar* es «descubrir o manifestar lo ignorado o secreto», mientras que *difundir* importa «propagar o divulgar». Es más, desde la perspectiva del objeto sobre el que recae la conducta, podría entenderse que revelar o difundir implica, conceptualmente, haber obtenido la información con anterioridad. Por tanto, si la obtención constituye un caso de agotamiento del espionaje informático, la revelación o difusión de los datos lo sería con mayor razón.

No obstante, es común que la revelación o difusión (indebida) de los datos también sea tipificada en forma autónoma, como ocurre en el artículo 4 de la Ley 19.223, que castiga «al que maliciosamente revele o difunda los datos contenidos en un sistema de información». En consecuencia, mientras que el espionaje informático supone una intromisión, en el sentido de que ha de existir un acceso a y conocimiento indebido de datos de un sistema informático, la revelación o difusión de los datos implica develarlos indebidamente respecto de terceros.

Espionaje, fraude y sabotaje informático

La relación entre el espionaje informático y las otras dos figuras paradigmáticas de la criminalidad informática, como son el fraude y sabotaje informático, se advierte en primer término si se analiza el objeto de la conducta en cuestión. Todos ellos han

de incidir en «datos informáticos», que el CCCE define como «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» (artículo 1 letra b). Además, como se dijo, cuando el comportamiento de cualquiera de esos delitos se lleva a cabo en el ciberespacio, ellos tienen un bien jurídico común, que corresponde a la «funcionalidad informática» (Mayer, 2017), sin perjuicio de la afectación de otros intereses públicos o privados. En fin, en tanto se trata de ilícitos que integran la delincuencia informática, comparten los elementos criminológicos de dicho sector de la criminalidad, entre ellos, las condiciones favorables que ofrece el ciberespacio para ejecutar conductas de forma anónima y transnacional (Miró, 2012: 152 y ss.), así como con efectos lesivos respecto de un gran número de potenciales víctimas (Sieber, 2014: 439).

En cuanto a la conducta incriminada, si partimos de la base de que el espionaje informático supone acceder a y conocer (indebidamente) datos de sistemas informáticos, constataremos que los delitos de fraude y sabotaje informático requieren que se verifique dicho acceso y eventual conocimiento. Así, en el caso del fraude informático, debe reconocerse que para alterar o manipular datos, a fin de causar un perjuicio patrimonial, ha de generarse un acceso y eventual conocimiento previo de tales datos. Tal situación provoca que el espionaje informático asuma la calidad de «delito presupuesto» del fraude informático.[19] Tratándose del sabotaje informático, cabe asimismo constatar que para destruir o inutilizar datos, debe verificarse un acceso y eventual conocimiento previo de dichos datos. Por tanto, en este caso también puede sostenerse que el espionaje informático presenta el carácter de «delito presupuesto» del sabotaje informático.[20]

Si se examina la relación concursal de los referidos ilícitos, convendría diferenciar aquella que se genera entre el espionaje y el sabotaje informático y la que se verifica entre el espionaje y el fraude informático. Respecto de la primera, considerando la sistemática de la Ley 19.223, que sugiere la consagración de figuras de aplicación alternativa; y las penas a imponer tanto al espionaje como al sabotaje informático, que no contemplan una regla expresa de acumulación aritmética, habría que plantear la existencia, al menos en la mayoría de los supuestos,[21] de un concurso de leyes, que

19. Se trata de una situación análoga a la que se verifica entre la mayoría de las lesiones corporales y el homicidio, en el sentido de que para matar en gran parte de los casos hay que herir, golpear o maltratar antes a la víctima. Véase Cury (2011: 670).

20. Con todo, ya que el conocimiento de los datos para la ejecución del fraude o sabotaje informático puede ser eventual, es posible que el vínculo se dé entre el fraude o sabotaje y una forma de ejecución imperfecta (tentativa) del espionaje informático.

21. En ese sentido, no puede descartarse el concurso medial entre el espionaje y el sabotaje informático, con eventual afectación de diversos bienes jurídicos, como cuando el agente debe primero acceder a los datos y conocerlos, para así definir cuáles serán objeto de destrucción o alteración.

se soluciona a favor del sabotaje informático en virtud del principio de absorción. En cuanto a la segunda, si se afirma que, a pesar de la inexistencia de una genuina hipótesis de fraude informático en el derecho chileno (véase Hernández, 2001: 16 y ss.), éste es subsumible en el sabotaje informático —en tanto importa modificación de datos—, cabría postular de nuevo un concurso de leyes, al menos en la mayoría de los casos,[22] entre el espionaje y el sabotaje informático, que se resolvería a favor de este último, de acuerdo con el principio de absorción.[23]

Espionaje informático y delitos contra la intimidad o privacidad

El nexo entre el espionaje informático y otros tipos de la parte especial puede plantearse, en primer término, respecto de los delitos del artículo 161-A inciso primero del Código Penal. Sabido es que los comportamientos allí sancionados se describen en términos relativamente amplios, pues contemplan verbos como «captar», «interceptar», «grabar», «reproducir», «sustraer», «filmar», «fotografiar». Del mismo modo, el objeto material de la conducta se expresa de forma bastante laxa, ya que ella puede recaer en «conversaciones», «comunicaciones», «documentos o instrumentos» e incluso en «hechos». En fin, si bien los medios de comisión respectivos no se hallan especificados en la ley —que, más aún, alude a «cualquier» medio—, ellos pueden inferirse en ciertos casos de las propias descripciones típicas. Así, por ejemplo, tratándose del comportamiento consistente en «fotografiar», es posible llevarlo a cabo a través de una cámara fotográfica, de un *smartphone* o de cualquier sistema de captación de imágenes análogo a ellos. Mientras que en otros supuestos, como la conducta consistente en «captar», el medio podría ser cualquiera capaz de registrar la conversación, comunicación, el documento o hecho de carácter privado.

Debido a la amplitud con la que aparece redactado el artículo 161-A inciso primero del Código Penal, es posible plantear su conexión con el delito de espionaje informático. En efecto, si entendemos que este último importa un acceso a y conocimiento indebido de datos, tal comportamiento podría implicar, por ejemplo, la captación o interceptación de documentos electrónicos, justamente, porque la extensión del tipo no se opone a ello. De otra parte, las conversaciones, comunicaciones o hechos pueden estar registrados en sistemas informáticos, lo que también origina puntos de contacto entre el espionaje informático y el delito del artículo 161-A inciso primero.

No puede obviarse, sin embargo, que dicho precepto contempla un elemento objetivo consistente en que el autor obre «sin autorización del afectado». Tal requisito no está expresamente previsto en el artículo 2 de la Ley 19.223 y, tratándose del CCCE,

22. Véase la nota 21.

23. En cambio, si se sostiene que el fraude informático es subsumible en el espionaje informático —en tanto supone acceso a datos—, no habría propiamente un concurso de leyes.

encuentra un reconocimiento en la infracción de medidas de seguridad cuya exigencia, según se dijo, sería facultativa (véase el artículo 2 CCCE y Hernández, 2020). Como veremos, es posible entender que, aun a falta de mención explícita, el espionaje informático supone la vulneración de barreras técnicas, que den cuenta de una expectativa de excluir a terceros del acceso a y conocimiento indebido de los datos. Con ello, otra vez se plantea un vínculo entre ambos ilícitos, en un caso por la opción prevista en el CCCE; en el otro, en virtud del desarrollo doctrinal.

Por último, el artículo 161-A inciso primero establece que el delito debe ejecutarse en «recintos particulares» o en «lugares que no sean de libre acceso al público». Según una interpretación restrictiva, tales alusiones podrían referirse a espacios físicos, circunstancia que excluiría cualquier conexión entre dicho ilícito y el espionaje informático, al menos cuando éste se comete en el ciberespacio. No obstante, de acuerdo con el sentido natural y obvio de los términos *recinto* y *lugar*, el primero corresponde a un «espacio, generalmente cerrado, comprendido dentro de ciertos límites», mientras que el segundo alude, en su primera acepción, a «porción de espacio». Se trata, según podrá advertirse, de definiciones sumamente amplias, que no se oponen a la consideración de *espacios virtuales* como internet. A su vez, cuando el legislador ha querido atribuir a la expresión *lugar* un sentido físico, más restringido que el indicado, lo ha hecho incluyendo, junto con la referencia al lugar, otras circunstancias, por ejemplo, que éste sea habitado o no habitado, como ocurre en algunas modalidades del robo (en ese sentido, Garrido, 2011: 234-235; Oliver, 2013: 217). Con todo, para que la idea de «espacio virtual» (Agustina, 2009: 1 y ss.) quede incluida en el sentido literal posible de «recintos particulares» o de «lugares que no sean de libre acceso al público», cobra especial relevancia que se hayan dispuesto barreras técnicas tendientes a restringir el ingreso de terceros, según indicaremos luego.

Los puntos de contacto entre el espionaje informático y las figuras del artículo 161-A inciso primero del Código Penal pueden dar lugar a hipótesis concursales. Piénsese, por ejemplo, en el sujeto que se encuentra de visita en la morada de la víctima e ingresa de forma subrepticia a un computador, en cuyo disco duro se almacenan imágenes íntimas de dicha víctima, que el agente graba en un *pendrive*. En tal caso, podría estimarse que se realiza tanto el tipo del artículo 161-A inciso primero del Código Penal, como el espionaje informático del artículo 2 de la Ley 19.223. Por su parte, si el acceso y conocimiento indebido se lleva a cabo de manera remota, mediante el uso de redes informáticas, también podrían verificarse los elementos típicos de ambos delitos.

La solución para esas dos hipótesis concursales difiere según cuáles sean los intereses afectados con la conducta. Así, en el evento en que sólo se incida negativamente en la intimidad del ofendido —lo que usualmente ocurrirá cuando no se actúe a través de internet—, existirá un concurso de leyes, que debería resolverse aplicando

el artículo 161-A inciso primero, por contemplar la pena más gravosa.[24] En cambio, si se afecta más de un bien jurídico, como la intimidad y la funcionalidad informática —lo que por lo general acontecerá si el delito se ejecuta mediante redes computacionales—, existirá un concurso ideal de delitos que, como se sabe, se resuelve aplicando la pena mayor asignada al delito más grave.

Asimismo, es posible plantear una relación entre el espionaje informático y el delito de violación de correspondencia del artículo 146 del Código Penal, en el entendido de que dentro de los datos que pueden ser objeto material del primero podría haber correspondencia electrónica. A pesar de que la noción de correspondencia es amplia, lo que desde un punto de vista semántico permitiría incluir también a la que se intercambia electrónicamente, una interpretación sistemática conduce a afirmar que ella sólo se refiere a la de carácter epistolar.[25]

Efectivamente, en el mismo párrafo en el que se regula dicho delito, más específicamente, en el artículo 156 del Código Penal, se prevé una figura agravada de violación de correspondencia, que sanciona a los empleados del Servicio de Correos y Telégrafos u otros que, prevaliéndose de su autoridad, cometan dicho comportamiento. Es evidente que la norma alude a la correspondencia contenida en papel, lo que excluye a la que está almacenada en servidores de correos electrónicos. Concluir algo distinto produciría consecuencias asistemáticas e injustificadas, como castigar con una pena agravada sólo la violación de correspondencia cuando ésta es epistolar, sin que exista una figura equivalente aplicable a los correos electrónicos. Ello supondría otorgar una protección penal mayor a la correspondencia contenida en papel que a la almacenada en sistemas informáticos, lo que no se aviene con la relevancia que actualmente tienen una y otra en tanto formas de comunicación de informaciones privadas.

De lo expresado puede colegirse que el delito de espionaje informático serviría para colmar el vacío que genera la regulación de la violación de correspondencia contemplada en el Código Penal. Lo dicho no obsta a la eventual aplicación de alguna de las figuras previstas en la Ley 18.168 (véase Couso, 2018: 43-44), concretamente en su artículo 36 B c), que castiga «al que intercepte o capte maliciosamente o grabe sin la debida autorización, cualquier tipo de señal que se emita a través de un servicio pú-

24. No obstante, como dicho ilícito contempla la pena de reclusión menor en cualquiera de sus grados, el juez podría considerar, al determinar su cuantía exacta (artículo 69 del Código Penal), el hecho de haberse verificado tanto el tipo del artículo 161-A inciso primero del Código Penal como el del artículo 2 de la Ley 19.223.

25. La doctrina tradicionalmente ha excluido la correspondencia electrónica como objeto material del delito del artículo 146 del Código Penal, pues el verbo *abrir* sólo sería aplicable a correspondencia contenida en papel. En esa línea, Etcheberry (2010a: 266) y Matus y Ramírez (2019: 225). A nuestro juicio, el sentido literal posible del verbo *abrir* no resulta vulnerado si se incluye la apertura de correos electrónicos. Con todo, existen motivos para no extender la conducta a esa clase de correos, según veremos *infra*.

blico de telecomunicaciones». En todo caso, dicho delito, como surge de su texto, se limita a los supuestos en que la información se capte mediante un servicio público de telecomunicaciones, lo que deja fuera a la gran mayoría de los servidores de correos electrónicos, por no constituir éstos un «servicio público». Por consiguiente, en los restantes casos sólo puede aplicarse el espionaje informático, sin que se produzcan vinculaciones entre éste y la violación de correspondencia.

Espionaje informático e información en el ámbito público (violación de secretos e infidelidad en la custodia de documentos)

El delito de espionaje (informático), como ha quedado de manifiesto, se relaciona con el concepto de «información», la que a su turno puede ser de diversas clases. Así, es posible hablar de información secreta o reservada,[26] que puede ser objeto material de varios ilícitos penales, en especial, de aquellos vinculados con la protección de la función pública y con ciertos hechos de relevancia pública. Entre dichos ilícitos se cuentan los distintos tipos de violación de secretos (artículos 246 a 247 bis del Código Penal) y de infidelidad en la custodia de documentos (artículos 242 a 245 del Código Penal).

Si bien la Constitución Política de la República consagra la publicidad de los actos y resoluciones de los órganos del Estado como una de las bases de la institucionalidad (artículo 8 inciso segundo de la Constitución), idea que se relaciona con el principio de transparencia de la actividad administrativa (Bermúdez y Mirosevic, 2008: 455), tal postulado tiene excepciones. El fundamento de ellas radica en la importancia del carácter secreto o reservado de determinadas informaciones del ámbito público para un correcto funcionamiento del aparato estatal (Rodríguez y Ossandón, 2011: 467-468), en tanto entidad al servicio de las personas (artículo 1 de la Constitución). Esto genera la necesidad de establecer tipos penales que sancionen el acceso indebido a ciertas informaciones (penalmente) relevantes y la difusión indebida de su contenido. Puesto que el espionaje (informático) implica un acceso a y conocimiento indebido de determinada información, es posible advertir un vínculo entre él y las figuras delictivas contra la función pública que pasaremos a examinar.

En lo que respecta a la violación de secretos, debe considerarse que el secreto se halla tutelado mediante una serie de delitos dispersos (véase Etcheberry, 2010b: 228; Labatut, 2012: 86), relativos a cuestiones tan variadas como la existencia de informa-

26. Algunos textos legales, como el artículo 21 de la Ley 20.285 sobre acceso a la información pública; y parte de la doctrina (véase García y Contreras, 2009: 153) emplean los vocablos información *secreta* y *reservada* como sinónimos. Sin embargo, existe normativa que hace importantes distingos entre ellos, destacando lo dispuesto en la p. 5 del Manual «de manejo y tramitación de la documentación del Estado Mayor de la defensa nacional», de 15 de febrero de 2008.

ción pública reservada, el secreto profesional, la prevaricación de abogados, etcétera.[27] Por ende, lo que el legislador denomina violación de secretos en el párrafo 8, título 5, libro 2 del Código Penal sólo alude a ciertas hipótesis en que el secreto resulta afectado, a saber, aquellas en que el agente es un funcionario o profesional universitario (Garrido, 2010: 476) actuando en su calidad de tal, que descubre un secreto público o de un particular, o que hace uso indebido de una información concreta y reservada. Como sea, los delitos que se relacionan en términos amplios con la violación de secretos tienen en común la idea de revelar o descubrir ciertas informaciones, cuya trascendencia puede afectar intereses públicos o privados.

El vínculo entre la violación de secretos y el espionaje (informático) se presenta de manera distinta a como podría pensarse *prima facie*, esto es, como un caso de agotamiento posterior al acceso a y conocimiento indebido de la información. En efecto, los tipos del párrafo 8, título 5, libro 2 del Código Penal y, en general, los que castigan el descubrimiento de secretos, parten de la base de que el agente integra el círculo de personas que puede acceder a la información cuyo conocimiento está limitado. Por tanto, dicho sujeto no requiere acceder indebidamente a la información, pues ella ya forma parte de su esfera de conocimiento.

Lo interesante del nexo entre ambos delitos radica en que el espionaje informático puede colmar lagunas de punición que se producen por la forma en que está regulada la violación de secretos. Como advierte la doctrina (Rodríguez y Ossandón, 2011: 471), la inexistencia de un tipo referido a la violación de secretos por parte de quien accede ilegítimamente a la información hace que dicho supuesto resulte impune, a pesar de su gravedad. En concreto, el espionaje informático podría llenar el vacío punitivo en aquellos casos en que un sujeto accede indebidamente a información secreta contenida en un sistema de tratamiento automatizado de la misma. De igual forma, ya que el tipo de espionaje informático no establece limitaciones en relación con el agente, ello permitiría ampliar la punibilidad más allá de los funcionarios o profesionales que actúan en calidad de tales, incluyendo, en general, a cualquiera que acceda a y conozca indebidamente información resguardada por el secreto. En suma, si bien el espionaje informático no sanciona específicamente el descubrimiento de tal información, sí posibilita el castigo para quienes de manera ilegítima accedan a ella y conozcan su contenido.

Una situación análoga se produce respecto del tipo del artículo 247 bis del Código Penal, que sanciona al empleado público que haga uso de un secreto o información concreta reservada, «de que tenga conocimiento en razón de su cargo» y obtenga un beneficio económico para sí o para un tercero. Como él puede ser cometido sólo por el funcionario que acceda a la información reservada en razón de su cargo, se excluye a otros funcionarios y, por cierto, a particulares que acceden de forma indebida a ella.

27. Un panorama respecto de tales conductas puede verse en Rodríguez y Ossandón (2011: 466-467).

De nuevo, si esa información se halla en un sistema de tratamiento automatizado y el agente ejecuta un acceso a y conocimiento ilegítimo de ella, podría aplicarse el tipo de espionaje informático, para así evitar la impunidad del comportamiento.

En cuanto al delito de infidelidad en la custodia de documentos, el vínculo más evidente que éste presenta con el espionaje informático concierne al tipo del artículo 244 del Código Penal, respecto de funcionarios públicos —así como también al del artículo 245, aplicable a particulares—, que castiga al que abriere o consintiere en que se abran papeles o documentos cerrados, cuya custodia le estuviere confiada —incluso de manera accidental—. Pues bien, a diferencia de lo que ocurre con la violación de secretos, aquí sí podría subsumirse el supuesto del funcionario (o particular) que accede indebidamente a la información mediante la apertura de los papeles o documentos cerrados.

No obstante, un problema que debe sortear la relación entre ambos delitos atañe al objeto material del tipo del artículo 244 del Código Penal, a saber, «papeles o documentos». En este contexto, si se siguiera una interpretación restrictiva de esas expresiones, o sea, que tales objetos sólo se refieren a soportes materiales, habría que concluir que se excluye al documento electrónico y a los datos informáticos, los que quedarían fuera de su órbita típica.

En cambio, si se adoptara una definición amplia de «papeles o documentos», sería posible sostener que en la voz *documentos* pueden subsumirse aquellos de carácter electrónico, atendido que el legislador contrapone el término *papeles* al de *documentos*. Justamente, la expresión *documentos*, según una interpretación progresiva (véase García-Pablos, 2014: 825), admite que no sólo los soportes contenidos en una materialidad, sino también los electrónicos e informáticos constituyan documentos. La esencia del carácter de documento radicaría, para esta tesis, antes que en su materialidad, en las funciones que él cumple al interior del tráfico jurídico, como son la perpetuación, garantía y prueba de ciertos hechos (García, 1997: 45 y ss.; Villacampa, 1999: 101-102).

Según el artículo 244 del Código Penal, tales documentos deben estar «cerrados», término que según su sentido natural y obvio puede interpretarse como disponer los documentos de modo que no sea posible ver lo que contienen. En el plano informático, es posible entender dicho requisito como equivalente a la existencia de barreras técnicas de acceso a los datos, cuya custodia tendría que haber sido confiada previamente a un funcionario.

Estimamos que esta interpretación no excede el sentido literal posible del precepto y tiene la ventaja de colmar, al menos en forma parcial, el vacío que genera el tipo de violación de secretos que, como se dijo, parte de la base de que el agente está facultado para acceder a la información que luego revela. Ahora bien, el vacío se colma parcialmente, ya que subsiste tratándose de documentos no electrónicos, pues, respecto de ellos, se mantiene la exigencia de que el funcionario (o particular) acceda de manera legítima a la información que se revela.

Por último, si se lleva a cabo un acceso indebido al contenido de un documento electrónico, a través de redes informáticas, se verificaría un concurso ideal entre el espionaje informático y la infidelidad en la custodia de documentos, toda vez que existiendo un hecho que satisface ambas descripciones, dichos delitos protegen bienes jurídicos distintos: en el primer caso, la funcionalidad informática y algún interés relacionado con el contenido de la información (por ejemplo, el patrimonio o la intimidad); en el segundo caso, aspectos operativos de la función pública, relativos a la reserva de ciertas informaciones (similar, Rodríguez y Ossandón, 2011: 482).

Espionaje informático e información en el ámbito privado (comunicación fraudulenta de secretos de fábrica y abuso de información privilegiada)

Como se ha reiterado, el espionaje informático tiene un estrecho vínculo con el uso de cierta información. Junto con las informaciones penalmente relevantes del ámbito público existen otras, de carácter privado, a las que el derecho penal también brinda tutela. Así ocurre, por ejemplo, respecto del tipo de comunicación fraudulenta de secretos de fábrica, del artículo 284 del Código Penal, y de las figuras que castigan el abuso de información privilegiada en la Ley 18.045.

El tipo del artículo 284 sanciona a quien «fraudulentamente hubiere comunicado secretos de la fábrica en que ha estado o está empleado». En cuanto a su objeto material, la expresión «secretos de fábrica» es interpretada como sinónimo de secretos de industria, los que a su vez se referirían «a las técnicas de fabricación, sea que consistan en máquinas o artificios originales, o en una disposición particular y diferente de elementos ya conocidos, etc.» (Etcheberry, 2010b: 278). En otras palabras, se otorgaría protección penal a los secretos de las denominadas «empresas fabriles o de producción», no así a los de las «empresas de servicios e intermediación», lo cual, ciertamente, provoca un vacío de punición (Acosta, 1988: 74-75). Algo parecido puede decirse en relación con los denominados «secretos de empresa», noción más moderna que comprendería, entre otras cosas, las listas de clientes (Fernández Díaz, 2018: 24). Dicho objeto material tampoco parece abarcado por el tipo del artículo 284 del Código Penal, lo cual nuevamente podría originar una laguna punitiva. Una manera de superarla, al menos cuando la información secreta está almacenada en un sistema de tratamiento automatizado de la misma, pasa por aplicar el delito de espionaje informático.

Según se infiere de la norma transcrita, a diferencia de lo planteado sobre la violación de secretos del funcionario, en que el acceso a la información debe producirse en virtud del desempeño (lícito) de la función pública, no ocurre lo mismo con el tipo de comunicación fraudulenta de secretos de fábrica. En ese sentido, los términos amplios en que aparece redactado el precepto permiten incluir al sujeto que ha accedido legítima o ilegítimamente a la información que luego comunica. En lo que aquí interesa, si

la información secreta de la fábrica está contenida en un sistema de tratamiento automatizado, al que el agente accede en forma indebida, habría, según los bienes jurídicos afectados y la eventual identidad material del hecho, un concurso de leyes o ideal, respectivamente, entre el espionaje informático y el tipo del artículo 284 del Código Penal.[28] En cambio, si el acceso a la información, aun cuando ella esté almacenada en un sistema informático, se hubiere verificado debidamente (por ejemplo, porque el hechor estaba facultado para ello), sólo sería aplicable la comunicación fraudulenta de secretos de fábrica, siempre que concurran sus restantes exigencias típicas.

En lo que atañe al abuso de información privilegiada, éste integra un grupo de delitos más amplio, tipificados en la Ley 18.045, que sancionan la revelación o el (ab)uso de información reservada o privilegiada (artículo 59 e, en relación con los artículos 85, 60 d, 60 e, 60 g y 60 h). Más allá de las particularidades de cada uno respecto del agente y de la conducta, todos tienen un objeto material común, a saber, información reservada o privilegiada,[29] de la que se hace un uso indebido.[30]

Las conexiones entre tales delitos y el espionaje informático pueden verificarse en la medida en que la información reservada o privilegiada esté en un sistema de tratamiento automatizado y el hechor acceda indebidamente a ella. Así, por ejemplo, si un sujeto accede de forma indebida a datos que corresponden a información privilegiada y luego se vale de ella para ejecutar un acto, por sí o por intermedio de otro, a fin de conseguir un beneficio económico o evitar una pérdida propia o ajena, mediante cualquier clase de operaciones o transacciones con valores de oferta pública, habría un concurso medial entre el espionaje informático y el tipo del artículo 60 g). Lo mismo podría decirse respecto del delito del artículo 60 h), que castiga al que revele información privilegiada, con el objeto de obtener un beneficio pecuniario o evitar una pérdida, tanto para sí como para un tercero, en operaciones o transacciones con valores de oferta pública. Ello se basa en que, existiendo dos hechos, se da entre ambos una relación de medio (espionaje informático) a fin (delito de la Ley 18.045).

Por el contrario, no se genera un nexo entre el espionaje informático y los tipos referidos cuando la información reservada o privilegiada no está contenida en un sistema informático. Tampoco existe relación entre tales ilícitos si la información ha sido obtenida por el sujeto en virtud de su calidad, o sea, lícitamente, como ocurre en la figura del artículo 60 d), que castiga a «los socios, administradores y, en general

28. Un análisis parecido puede encontrarse en Corcoy (2007: 21-22). Habrá un concurso de leyes si, por ejemplo, sólo se incide negativamente en intereses patrimoniales; mientras que habrá un concurso ideal si, existiendo un hecho que satisface ambas descripciones, el comportamiento se realiza a través de redes informáticas y, con ello, se afecta además la funcionalidad informática.

29. Véase, respecto de información «no pública», García (2013: 25); y de información «asimétricamente repartida», Perrone (2009: 198).

30. En el entendido de que la revelación implica, de cierta forma, un uso (indebido) de la información.

cualquier persona que en razón de su cargo o posición en las sociedades clasificadoras, tenga acceso a información reservada de los emisores clasificados y revele el contenido de dicha información a terceros».

Espionaje informático y delitos contra la propiedad intelectual o industrial

También es posible plantear un vínculo entre el espionaje informático y las figuras delictivas que afectan a la propiedad intelectual o industrial. En cuanto a las primeras, resultan relevantes, entre otros,[31] los tipos del artículo 79 letras a) y b) de la Ley 17.336, según los cuales, comete falta o delito contra la propiedad intelectual, respectivamente, «el que, sin estar expresamente facultado para ello, utilice obras de dominio ajeno protegidas por esta ley, inéditas o publicadas, en cualquiera de las formas o por cualquiera de los medios establecidos en el artículo 18»;[32] así como «el que, sin estar expresamente facultado para ello, utilice las interpretaciones, producciones y emisiones protegidas de los titulares de los derechos conexos, con cualquiera de los fines o por cualquiera de los medios establecidos en el t*ítulo* 2» (que regula los derechos conexos al derecho de autor).

La relación entre el espionaje informático y los delitos contra la propiedad intelectual viene dada porque las obras de dominio ajeno tuteladas por la ley, o las interpretaciones, producciones y emisiones protegidas de los titulares de los derechos conexos, que constituyen su objeto material, pueden hallarse en un soporte informático (véase Grunewaldt, 2013: 96). A su turno, es posible que un individuo acceda indebidamente al sistema de tratamiento automatizado en que los datos están contenidos. En tal evento se verificaría un concurso medial entre el espionaje informático y el delito contra la propiedad intelectual de que se trate, pues, existiendo dos hechos, se da entre ellos un vínculo de medio (espionaje informático) a fin (delito de la Ley 17.336).

En lo que respecta al nexo entre el espionaje informático y los delitos que afectan a la propiedad industrial, se verifica una situación similar a la descrita. Efectivamente, si consideramos, por ejemplo, los tipos del artículo 52 de la Ley 19.039, ellos castigan, entre otras cosas, a los que maliciosamente utilicen en el comercio un invento patentado o estén en posesión del mismo (letra a); así como a los que maliciosamente, con fines comerciales, hagan uso de un procedimiento patentado (letra c). O sea, se trata de ilícitos que, de recaer en un objeto material almacenado en un sistema de tratamiento automatizado de la información, podrían implicar la comisión de un espionaje informático. En tal caso habría, por las mismas razones indicadas *supra*, un concurso medial entre el espionaje informático y el delito contra la propiedad in-

31. A ellos pueden agregarse los del artículo 79 bis u 80 a) de la Ley 17.336.

32. Norma que establece las formas según las cuales el titular del derecho o autor, o quienes estuvieren expresamente autorizados por él, tendrán la facultad de utilizar la obra.

dustrial en cuestión. Para ello sería necesario que el agente accediera indebidamente a datos contenidos en dicho sistema, en los que se encuentre alguno de los objetos materiales aludidos.

Dificultades que enfrenta el castigo del espionaje informático en el plano dogmático

El injusto específico del espionaje informático y la información como clave para explicarlo

Como es sabido, vivimos en una sociedad de la información, que podemos definir como aquella clase de organización social en que la información, así como las tecnologías que operan sobre ella (Torres, 2017: 11-12; con énfasis en internet, Flores, Galicia y Sánchez, 2007: 20-21), ocupan un lugar sustantivo y atraviesan todas las actividades (educación, servicios, entretenimiento, comercio, industria, etcétera) (Crovi, 2002: 16). Justamente, la importancia social que tiene la información ha llevado a que se la regule a través de un conjunto de normas, cuyo alcance dependerá del contenido de ella. A partir de esa normativa, surgen tensiones entre la disponibilidad y el libre intercambio de la información, por una parte, y la necesidad de establecer límites y sanciones, incluso penales, para los comportamientos que vulneran intereses subyacentes a ella, por la otra (similar, Marti y Vega-Almeida, 2005: 41).

Desde un punto de vista penal, no puede soslayarse que atendida la utilidad social que reviste la disponibilidad y el libre intercambio de la información, el ámbito del denominado «riesgo permitido» (Roxin, 2006: 382) es considerablemente amplio. Ello implica que un gran número de conductas vinculadas con el acceso a la información, así como con su tratamiento y transferencia, no será objeto de sanción penal (de forma análoga, Medina, 2014: 81). Antes bien, su castigo punitivo sólo resultará racional cuando nos hallemos ante graves ataques de intereses de gran relevancia social o «bienes jurídicos» (Mir, 2016: 128 y ss.), sean de carácter individual o colectivo.

A partir de esta última sistematización de los intereses que subyacen a la información a la que se accede, o que se almacena o transmite, es posible identificar una extensa gama de comportamientos punibles, relacionados con los delitos informáticos *stricto sensu* (espionaje, sabotaje y fraude informático) (véase Mayer, 2017: 237). En atención al objeto del presente trabajo, la conducta consistente en acceder a información contenida en sistemas informáticos es la que concitará nuestro interés, en la medida en que ella involucre un actuar indebido, que traspase la barrera del riesgo permitido. La conjugación de los elementos antes referidos posibilita delinear el injusto del delito de espionaje informático, en el sentido que pasaremos a desarrollar.

Según se esbozó, las informaciones almacenadas en sistemas informáticos —o «datos informáticos»— pueden vincularse con intereses individuales, como la inti-

midad o el patrimonio; o colectivos, como la función pública o la seguridad nacional. Si partimos de la base de que la importancia del bien jurídico y su nivel de afectación constituyen baremos relacionados con la gravedad del delito, en el caso del espionaje informático sería posible distinguir niveles de intensidad del injusto. En ese orden de ideas, no es indiferente que con él se afecte uno o varios bienes jurídicos, es decir, que el delito sea pluriofensivo. En paralelo, tendrá que considerarse la naturaleza y relevancia del interés vulnerado e incluso la peligrosidad que el comportamiento entraña para otros bienes jurídicos.

Respecto de la naturaleza e importancia del interés conculcado, no puede tener una valoración equivalente, en términos de su gravedad, un espionaje informático relativo a los datos para acceder a la banca en línea de un cliente en particular, que aquel que recae en informaciones militares, que comprometen la seguridad de toda la nación.[33] En este último caso, ya que se afecta un presupuesto fundamental para el disfrute de los restantes bienes jurídicos, la vulneración del bien jurídico resultará de extrema gravedad y explicará la alta penalidad con la que se sanciona el espionaje de informaciones militares, que puede llegar incluso al presidio perpetuo (artículo 109 del Código Penal).

Por su parte, existen supuestos en que el espionaje informático referido a información pública reservada —por ejemplo, administrativa o judicial— será más grave que el que recae en información íntima de una persona concreta. Además, es posible que dicha información pública se vincule con intereses de titularidad de los individuos que interactúan en esos ámbitos (por ejemplo, su honor). Por ende, a pesar de que a primera vista podría estimarse que la afectación de un bien jurídico individual, como la intimidad, es más disvaliosa que la vulneración de la función pública o jurisdiccional, esta última puede ir unida a la afectación de intereses individuales, lo que le confiere un *plus* de gravedad. Asimismo, no puede obviarse que el espionaje informático cometido por un funcionario respecto de tales informaciones también transgrede los deberes que éste tiene en el desarrollo de su función (en esa dirección, Rodríguez y Ossandón, 2011: 99), cuestión que puede implicar un mayor desvalor de resultado.

La existencia de barreras técnicas como señal de exclusión inequívoca de terceros

En la sociedad de la información, en especial de la que está disponible en el ciberespacio, lo usual será el libre acceso a datos por parte de cualquier individuo y en todo momento. En este ámbito se verificarán los casos de riesgo permitido ya referidos, lo que supone, en concreto, que acceder a las informaciones disponibles en internet

33. A propósito de esta materia, Lara, Martínez y Viollier (2014: 110-111) critican que el artículo 2 de la Ley 19.223 no establezca criterios relativos a la mayor o menor importancia de los datos afectados.

no conllevará sanciones penales. Tras esta idea está otra, más general, según la cual quienes interactúan en el ciberespacio lo hacen en una suerte de contexto sin fronteras (Pineda y otros, 2003: 258), en que el conocimiento se encuentra asequible para todo aquel que quiera alcanzarlo. Sin embargo, como suele ocurrir cuando están en juego los intereses de terceros, la libertad para acceder a informaciones disponibles en internet no es absoluta.

En este contexto, surge la pregunta relativa a si la tutela punitiva va a extenderse a todos quienes, siendo titulares o encargados de la información, no han consentido en que ella sea objeto de intromisiones; o si, en cambio, la protección penal abarcará únicamente a quien estableció barreras técnicas de acceso a la misma.[34] La primera posibilidad tiene la ventaja de generar una amplia tutela de los datos, no obstante, a un costo difícil de conciliar con la necesaria certeza que ha de existir en materia punitiva. En ese sentido, la disposición de barreras técnicas, aunque acota la protección penal únicamente a las informaciones que se hallan así resguardadas,[35] constituye una señal de exclusión inequívoca de terceros (véase Medina, 2014: 89), lo que permite escapar del subjetivismo a que podría conducir el hecho de hacer depender la realización del tipo de una voluntad del titular o encargado de la información, que no ha sido exteriorizada a través de algún mecanismo de seguridad.

Podría objetarse a este planteamiento la circunstancia de demandar una exigencia no prevista explícitamente en la Ley 19.223, que además pone de cargo de la víctima la tutela de sus propios bienes jurídicos, situación que no se verificaría respecto de otros delitos. Para enfrentar esta crítica, debe considerarse que la realización del tipo supone, entre otras cosas, que el agente sepa que está llevando a cabo una conducta punible, en este caso, de espionaje informático, y, para ello, en el contexto comisivo que analizamos —paradigmáticamente, internet— no basta la mera ausencia de voluntad del ofendido. Mucho menos en una sociedad, como la nuestra, caracterizada por la disponibilidad y el libre intercambio de la información, según lo planteado *supra*.

Tratándose de datos ligados con bienes jurídicos individuales, como información íntima o personal, usualmente será su propio titular quien establezca barreras técnicas que excluyan a terceros. Ellas pueden consistir en claves de seguridad (Huerta y Líbano, 1996: 258; Hernández, 2020), control de acceso mediante huella digital (Medina, 2014: 88), reconocimiento facial u otros. En estos supuestos, el acceso a la informa-

34. Esta alternativa se consagra expresamente en el artículo 36 B e) inciso final de la Ley 18.168, que, a propósito de la figura de distribución no autorizada de señales, establece: «Se considerará, para estos efectos, que la señal satelital se encuentra adecuadamente protegida si es que el permisionario del servicio ha adoptado, oportunamente, medidas tecnológicas suficientes para el resguardo de sus servicios».

35. En esa dirección, con referencia a la disposición de mecanismos de autentificación y a la vulneración de la confidencialidad de los datos por parte de quien infringe dicha barrera técnica, Brodowski (2019: 55).

ción, que dará origen a un espionaje informático en tanto acceso a y conocimiento indebido de datos, implicará actuar sin o contra la voluntad de su titular. Asimismo, la disposición de barreras técnicas operará como manifestación de una voluntad de exclusión de otros. Como contrapartida, el no establecimiento de tales barreras actuará como expresión de una voluntad de tolerancia del acceso a los datos que no estén protegidos (similar, Winter, 2013: 281-282), lo que impedirá la perpetración de aquel ilícito.[36] Frente a ello, la mera declaración unilateral o aun la existencia de una convención tendiente a excluir a otros no sería suficiente ni otorgaría la certeza que requiere el comportamiento penalmente relevante (en esa línea, Medina, 2014: 94-95).[37]

Así, por ejemplo, si un sujeto almacena imágenes íntimas en las que él figura, el establecimiento de un sistema de control de acceso a los archivos que las contienen, mediante reconocimiento facial, constituye un signo inequívoco de exclusión de otros a dicho material (Medina, 2014: 97). En cambio, si ese mismo individuo aloja las imágenes en un blog abierto o en el que, por ejemplo, sólo se han dispuesto condiciones de uso del sitio web que las aloja, se vuelve a la regla general, o sea, de libre acceso a los datos. Por su parte, si un sujeto emplea un nombre de usuario y clave de seguridad para ingresar a su sistema de banca en línea, está manifestando su voluntad de excluir a terceros. Mientras que si pone a disposición de otros —no obligados por el secreto o la reserva— su nombre de usuario y clave de seguridad, por ejemplo, en una red social, se vuelve a la regla de libre acceso a la información.

Tratándose de datos vinculados con intereses colectivos, es posible que el establecimiento de barreras técnicas se relacione con ciertos deberes de custodia de la información. En términos análogos a los deberes extrapenales que subyacen a delitos como el de infidelidad en la custodia de documentos (artículos 242 a 245 del Código Penal), puede que exista un sujeto (paradigmáticamente, un funcionario) a cargo de resguardar la información, cuestión que implica, ciertamente, disponer medidas (técnicas) —más o menos sofisticadas— tendientes a impedir que terceros no autorizados accedan a ella. En dicho evento, el establecimiento de barreras técnicas opera como señal inequívoca de la exclusión de sujetos ajenos al sistema, mientras que el hecho de no disponerlas puede acarrear responsabilidad (civil, administrativa e incluso penal) para quien no ha custodiado adecuadamente la información a su cargo.

36. En ese caso, se verifica una situación equivalente a la del delito de violación de morada (artículo 144 del Código Penal), que castiga al que entrare en morada ajena contra la voluntad de su morador (véase Labatut, 2012: 35). No obstante, para su configuración no cabe exigir la existencia de límites que supongan un «obstáculo efectivo» para el acceso de terceros (así, en cambio, Escalona, 2004: 157; Morón, 2007a: 105), pues ello podría privar de tutela a personas que, por ejemplo, por razones culturales o económicas carecen de aquéllos, cuestión que no se justifica dogmática ni político-criminalmente.

37. Tales supuestos incluirían el establecimiento de condiciones de uso del sistema que no involucran medidas —y menos barreras— técnicas, como *terms of service*, *terms of use* o *terms and conditions* (Hernández: 2020).

Más allá de que el establecimiento de barreras técnicas de acceso a los datos pueda sustentarse en normas extrapenales relativas a los deberes de custodia de ciertas informaciones, su disposición constituye un criterio objetivo para la interpretación del comportamiento penalmente relevante en el ámbito del espionaje informático. No en vano, dos de los principales ordenamientos jurídicos que suelen ser considerados a la hora de introducir reformas a la normativa penal chilena, como son el alemán y el español, contemplan la superación o vulneración de medidas de seguridad en la descripción típica de dicho delito.[38] Frente a ello, según se destacó *supra*, el CCCE establece la disposición de tales medidas como una *facultad* de los Estados parte (Hernández: 2020), lo que puede impactar negativamente en su consagración expresa por parte de todos los países que lo han suscrito.

La relevancia jurídico-penal del espionaje informático

Un asunto que suele generar dificultades al delimitar el injusto de las figuras que integran la criminalidad informática es el de la significancia penal de los comportamientos. Para graficarlo, una hipótesis en que la relevancia típica sería sumamente dudosa es, por ejemplo, la del sabotaje informático que importa destruir datos respaldados en otros soportes y que, por ende, pueden recuperarse fácilmente por su titular; o bien, referente a datos informáticos que cuantitativa o cualitativamente resultan insignificantes, por ejemplo, porque por su número o carácter no son capaces de dar cuenta de informaciones penalmente relevantes.[39]

En el delito de espionaje informático también pueden plantearse hipótesis de falta de significancia penal, en las que, si bien se verifica un acceso formalmente indebido, en el que ha existido, por ejemplo, vulneración de barreras técnicas, de todos modos no es posible identificar una afectación relevante de los bienes jurídicos subyacentes a la conducta. Tal podría ser el caso de un particular que ingresa indebidamente a la base de datos del Departamento de Evaluación, Medición y Registro Educacional (DEMRE) para conocer sus resultados de la Prueba de Selección Universitaria (PSU) horas antes de que ellos sean publicados. En tal evento, a pesar de que podría afirmarse una afectación de la funcionalidad informática,[40] no se divisa la vulneración de otros intereses, razón que lleva a postular la falta de necesidad de castigo punitivo,[41]

38. Véase el § 202a del StGB y el artículo 197 bis del Código Penal español.

39. Así, por ejemplo, la destrucción de una receta de cocina (Jijena, 1994: 362) o de aplicaciones en desuso contenidas en un sistema informático.

40. Por ejemplo, porque se ha incidido negativamente en la seguridad en el uso de redes informáticas.

41. Si la conducta fuese cometida por un funcionario podría plantearse la vulneración de sus deberes como tal y serviría para fundamentar su castigo por anticipación indebida de información (artículo 246 inciso final del Código Penal).

al menos a título de espionaje informático.[42] Asimismo, pueden plantearse casos en que se accede indebidamente a datos que cuantitativa o cualitativamente resultan insignificantes, por ejemplo, si se ingresa a un computador en el que no se almacena información penalmente relevante en atención a los intereses subyacentes a ella.

Lo dicho no es sino una aplicación de uno de los postulados de la teoría de la imputación objetiva, como es el principio de insignificancia penal.[43] Sabido es que, según éste, ha de excluirse la imputación objetiva cuando la conducta cree un riesgo irrelevante para el bien jurídico (Velásquez, 2009: 686). En tales hipótesis, aunque es posible sostener que el comportamiento ha generado o aumentado un riesgo para el objeto de protección penal, lo ha hecho de una manera intrascendente, motivo que lleva a descartar el castigo punitivo. Pues bien, en los supuestos señalados, a pesar de haberse verificado un acceso (indebido) a los datos, el desvalor de resultado que él implica, respecto de los intereses vinculados con la información a la que se ha accedido, carece de la entidad suficiente para fundar la imputación objetiva por un espionaje informático.

En cambio, en el plano subjetivo, un primer problema lo genera la eventual responsabilidad culposa. A nuestro juicio, existen razones para rechazar el castigo del espionaje informático a ese título: primero, ello no sería coherente con el principio de fragmentariedad penal que, como se sabe, impone sancionar los atentados más graves contra los bienes jurídicos más relevantes; segundo, ello no se justificaría sistemáticamente si tenemos en cuenta los diversos delitos que tienen por objeto información penalmente relevante, analizados *supra*, que prevén el castigo a título doloso y no culposo. A lo anterior se agrega que la vulneración de barreras técnicas de acceso a los datos no resulta concebible, sino con intención, o sea, con dolo (Picotti, 2013: 87).

Desde el punto de vista de esta última disposición anímica, no obstante que la fenomenología de la criminalidad informática parece hablar a favor de la exigencia de dolo directo respecto de las distintas figuras penales que la integran, es posible imaginar supuestos de espionaje informático en los que el agente actúe con dolo eventual. Así, por ejemplo, podría ocurrir que un sujeto se represente como probable que el medio que emplea, a fin de acceder indebidamente a un sistema informático, es idóneo para conocer la información en él almacenada y cuente con ello al ejecutar la conducta. Según nuestra opinión, si el hecho se realiza a través de internet debiese resultar punible, en atención a que el desvalor de resultado subyacente a la conducta es alto.[44] Sin embargo, tal necesidad objetiva de pena podría verse obstaculizada si

42. Lo que es sin perjuicio de su sanción a otro título. Véanse los dos acápites siguientes.

43. Por su parte, Malamud (2018: 156, 161) relaciona la gravedad de la conducta con los principios de mínima intervención y subsidiariedad, y plantea la inconveniencia de incluir expresamente una exigencia referida a la gravedad del hecho, a propósito del sabotaje informático.

44. Véase la sección «El injusto específico del espionaje informático y la información como clave para explicarlo».

subjetivamente y, según veremos, se incorporan referencias al ánimo o a las motivaciones del autor, cuya concurrencia suele asociarse —a nuestro juicio, sin fundamentos suficientes— con el dolo directo.

Bases para la (eventual) (re)tipificación del espionaje informático

Más allá de las dificultades que el espionaje informático genera, sobre todo en el plano conceptual y de su delimitación respecto de otros ilícitos, su actual regulación en la Ley 19.223 también es fuente de diversos inconvenientes que deberían ser revisados en una futura reforma legislativa.

Dicho delito está tipificado en el artículo 2 de la Ley 19.223, que castiga al 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». Tal descripción difiere de la que se contempla en el CCCE que, junto con establecer en su artículo 2 un deber de regulación del «acceso deliberado e ilegítimo a todo o parte de un sistema informático», dispone que los Estados parte de dicho convenio podrán exigir que el delito se lleve a cabo «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».

El tipo del artículo 2 de la Ley 19.223 presenta algunos problemas de técnica legislativa y de aplicación práctica, que llevan a sugerir cambios a su redacción. En concreto, no parece adecuado regular, junto con el acceso, comportamientos que más se acercan al sabotaje informático, como los consistentes en interceptar el sistema de tratamiento de la información o —sobre todo— interferir en él. Por otro lado, la consagración de un elemento subjetivo del injusto, como es el ánimo de apoderarse, usar o conocer indebidamente la información contenida en el sistema, no resulta justificada (Magliona y López, 1999: 166-167) si se considera que lo decisivo en el espionaje informático es actuar con el dolo de acceder a y conocer indebidamente la información del sistema. Desde este punto de vista, la exigencia expresa de dicho ánimo entorpece de manera innecesaria la aplicación práctica de la figura (Londoño, 2004: 176),[45] toda vez que impone acreditar un elemento subjetivo, que no se relaciona con las características esenciales del espionaje informático.[46]

Frente a ello, las directrices del CCCE resultan más apropiadas, en especial las que plantean tipificar como delito el acceso ilegítimo a un sistema informático. Con todo,

45. Un razonamiento parecido respecto del descubrimiento de los secretos de empresa puede encontrarse en Morón (2007b: 135-136, n. 53).

46. En ese sentido, estamos de acuerdo con el planteamiento de Flor (2012: 126), quien entiende que el núcleo del injusto, en este caso, radica en la vulneración del derecho de exclusión del titular del sistema informático, independiente de los motivos o propósitos perseguidos por el agente de la conducta típica.

ellas pueden provocar inconvenientes relativos al requisito facultativo consistente en infringir medidas de seguridad o a la declaración del Estado chileno en orden a demandar una intención delictiva determinada en el agente.[47]

En cuanto a lo primero, el hecho de consagrar expresamente, a nivel típico, la superación de barreras técnicas aporta un criterio objetivo para la delimitación del comportamiento penalmente relevante y confiere mayor certeza a la interpretación de la figura. Por ello, sería deseable que tal exigencia se contemplara de manera explícita en una futura reforma legal del espionaje informático.

En cuanto a lo segundo, el Estado chileno estableció una declaración al CCCE, consistente en que se exija «una intención delictiva determinada» en el autor, «conforme lo requiere el artículo 2 de la Ley 19.223 sobre delitos informáticos». Tal exigencia no parece conveniente, sea que se la interprete en relación con el dolo o como un «ánimo de […] conocer indebidamente de la información contenida en un sistema de tratamiento de la misma».

De un lado, a quienes acceden a un sistema informático de terceros les son aplicables las reglas generales en materia de eximentes de responsabilidad penal (véase Londoño, 2004); consiguientemente, si el acceso se lleva a cabo mediando la voluntad favorable del titular o encargado de los datos, no podría hablarse de un acceso ilegítimo o indebido, sino todo lo contrario.

De otro lado, quienes acceden a un sistema informático ajeno pueden hallarse en un supuesto de *hacking* puro o blanco, en que se verificaría un mero acceso a datos o programas, por ejemplo, para demostrar las vulnerabilidades del sistema (Miró, 2012: 55), hipótesis también denominada *hacking* ético (véase Jamil y Khan, 2011; Smith, Yurcik y Doos, 2002). A nuestro juicio, en tanto ese supuesto no incide negativamente en algún interés subyacente a información a la que se accede y que se conoce, él no podría calificarse de *espionaje informático* ni, por ende, regularse en el marco del mismo. Con todo, al tratarse de una conducta que implica la vulneración de un sistema informático, ella debería castigarse penalmente, pero mediante una figura específica que sancione el simple acceso a un sistema informático, así como con una pena muy inferior a la del espionaje.

En relación con este último tema, según lo señalado, el delito de espionaje informático debería poder satisfacerse con dolo eventual, como cuando el agente se representa como probable que el medio que utiliza, a fin de acceder indebidamente a un sistema informático, es idóneo para conocer la información en él almacenada y cuenta con ello al ejecutar la conducta. Lo anterior confirma que, para dar cuenta de su injusto, no resulta necesaria cláusula alguna que apunte a un reforzamiento del elemento subjetivo.

En otro orden de cosas, no estimamos indispensable que se aluda expresamen-

47. Véase, en el CCCE, la declaración de la letra a).

te a la significancia jurídico-penal del comportamiento. Incluso más: su referencia explícita podría acarrear consecuencias indeseables en el plano interpretativo. Por una parte, ello puede entenderse como una aplicación de los postulados de la teoría de la imputación objetiva y, más precisamente, de aquellos que tienden a precisar qué conductas son típicamente relevantes. Por otra parte, desde un punto de vista sistemático, establecer una exigencia expresa de significancia en el espionaje informático podría provocar que se prescinda de ella en todos aquellos delitos que no la consagren en su descripción legal, cuestión que podría generar interpretaciones muy amplias de los comportamientos a ser sancionados.

Por último, teniendo en cuenta las penas de la Ley 19.223, consideramos que debería revisarse la sanción aplicable al espionaje informático, ya que son imaginables supuestos en los que sea más grave acceder a y conocer indebidamente datos que, por ejemplo, destruirlos. En esta materia resulta decisiva la clase de información concernida, pero también los efectos que la conducta genera respecto de ella.

Propuesta de regulación del denominado «acceso ilícito» en actual trámite parlamentario (artículo 2 del Boletín 12.192-25)

El proyecto de ley que pretende reformar la tipificación de los delitos informáticos (Boletín 12.192-25) planteó regular el espionaje informático bajo el *nomen iuris* de «acceso ilícito». En la tramitación parlamentaria, el precepto propuesto en un principio fue objeto de modificaciones, encontrándose actualmente aprobado el siguiente texto:

> Artículo 2. Acceso ilícito. El que, sin autorización o de forma deliberada e ilegítima y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.
>
> Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en su grado mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.
>
> En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo.

La iniciativa transcrita consagra, en realidad, cuatro tipos penales:

En primer lugar, el *hacking* o mero acceso indebido a un sistema informático. Con él se castigaría el simple hecho de ingresar a un sistema informático, sin contar con autorización para ello, o bien, actuando de manera deliberada e ilegítima, y vulnerando barreras técnicas o medidas tecnológicas de seguridad. En ese sentido, se opta por consagrar explícitamente la superación de tales barreras, en tanto señal

inequívoca de exclusión de terceros, decisión que tiene la ventaja de establecer un elemento típico que, con altos grados de objetividad y certeza, circunscribe el ámbito de lo punible.

En cuanto a la técnica legislativa, la norma propuesta plantea, en términos alternativos, dos modalidades ejecutivas, una de carácter objetivo y otra de índole subjetiva, a saber: obrar sin autorización,[48] o hacerlo de forma deliberada e ilegítima. Se trata de una descripción poco recomendable, no sólo porque mezcla los planos objetivo y subjetivo a nivel comisivo, sino porque podría llevar a pensar que quien actúa sin autorización no necesariamente lo hace de manera deliberada e ilegítima. Tampoco es clara la necesidad de aludir, alternativamente, a «barreras técnicas» o «medidas tecnológicas de seguridad» y, más bien, habría sido preferible optar por una única cláusula que apuntara a esa idea.

En el plano dogmático, el hecho de aludir a una eventual «autorización» para ingresar al sistema podría interpretarse, en principio, como una exigencia que excluye la antijuridicidad del hecho. No obstante, atendida la redacción de la propuesta, es posible entender que contar con dicha autorización equivale a que concurra la voluntad del titular o encargado del sistema informático. Si se parte de esa base, la cláusula en comento permitiría excluir la tipicidad, en términos análogos a lo que ocurre cuando, por ejemplo, concurre la voluntad de la potencial víctima de una conducta constitutiva de hurto o violación.

La pena para este supuesto es baja (presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales), lo que resulta coherente con que el comportamiento más lesivo en este ámbito sea el espionaje informático, o sea, una conducta que involucra conocer la información contenida en el sistema, y no el simple acceso no autorizado. En paralelo, dicho castigo, que podría ser sólo pecuniario, confirma que el legislador está del lado de quienes entienden que la intromisión en sistemas informáticos ajenos no tiene cabida, al menos no en el marco de la legalidad.

En segundo lugar, se contempla un tipo que se acerca a lo que aquí hemos denominado espionaje informático, pero que sigue cargando con un elemento similar al previsto en el artículo 2 de la Ley 19.223, que limita innecesariamente su aplicación: «el ánimo de apoderarse o usar la información contenida en el sistema informático». Sorprende que no exista referencia, como sí la hay en el aludido artículo 2, al «ánimo de […] conocer indebidamente de la información contenida en un sistema de tratamiento de la misma». A propósito de este punto, aunque «conocer» podría quedar captado en «apoderarse» o «usar», también cabe entender que no se contempló claramente aquella alternativa típica.

48. Esta expresión es amplia, y podría abarcar tanto el comportamiento de un *outsider*, que actuaría, propiamente, sin autorización; como el de un *insider*, que actuaría excediendo la autorización que posee. Sobre ello, véase Karagiannopoulos (2018: 117).

En concordancia con lo ya expresado, la exigencia de un ánimo especial no se justifica y más bien augura una escasa aplicación práctica del delito. En este contexto, mejor habría sido regular, simplemente, el acceso a y conocimiento indebido de datos, para lo cual bastaría el dolo y no se necesitaría una tendencia interna trascendente adicional. Asimismo, demandar un ánimo como el mencionado puede ocasionar que se termine castigando una hipótesis de auténtico espionaje informático recurriendo al tipo del inciso primero (*hacking* o mero acceso indebido), con el riesgo de imponerle al agente una penalidad menor que aquella que le habría correspondido, considerando la mayor gravedad del hecho.

En tercer lugar, se establece la misma pena de la figura anterior para quien «divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste». En la línea de la regulación del uso de documentos falsos (artículos 196 y 198 del Código Penal), se eleva a la categoría de tipo autónomo un comportamiento que constituye una fase de agotamiento del espionaje informático. Con ello, además, se está incluyendo una conducta análoga a la del artículo 4 de la Ley 19.223, que sanciona al que «maliciosamente revele o difunda los datos contenidos en un sistema de información», pero, en este caso, sin exigir malicia, lo que puede contribuir a una mayor aplicación del precepto.

En cuarto lugar, se prevé una hipótesis calificada aplicable a quien, copulativamente, obtenga y divulgue la información, pues, en tal evento, el castigo sería presidio menor en sus grados medio a máximo. Esta sanción, como ocurre con las figuras de los artículos 2 y 4 de la Ley 19.223, sigue ubicando al ilícito en el ámbito del simple delito, cuestión que resulta razonable en supuestos ordinarios, no así, por ejemplo, cuando la información sea altamente sensible o ponga incluso en riesgo la seguridad nacional, en cuyo caso tendría que preferirse un tipo más específico, justamente, por la especialidad de la información comprometida con el comportamiento.

El artículo 2 debe complementarse con el artículo 16, según el cual: «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 mediando la autorización expresa del titular del mismo». Como podrá notarse, dicho texto echa por tierra las pretensiones de excluir del castigo al *hacking* puro o blanco, así como al ético, en términos que poco espacio dejan a una interpretación contraria.

Efectivamente, la necesidad de contar con una autorización expresa del titular del sistema impide prescindir de la pena si es que ha mediado una voluntad tácita o meramente presunta del mismo. Tal voluntad, cuya presencia podría haberse afirmado ante la tolerancia de ingreso al sistema informático, ha quedado claramente descartada y, en cambio, sólo se acepta el acceso al sistema si ha existido una autorización explícita en ese sentido. Por tanto, para definir el ámbito de lo punible, el legislador no toma en cuenta la motivación o finalidad de quien ingresa al sistema sin autori-

zación —que podría ir desde el genuino altruismo hasta el efectivo menoscabo—, sino que el hecho de que el titular hubiere o no concedido tal autorización. Así, se confirma la tendencia apuntada *supra*, de que el acceso no autorizado a sistemas informáticos involucra una afectación de intereses penalmente relevantes merecedora de castigo penal.

Esta forma de enfrentar el tratamiento punitivo del *hacking*, en especial del puro o blanco, o ético, ha sido resistida por quienes entienden que su criminalización podría afectar el desarrollo de la ciberseguridad, en particular la detección de vulnerabilidades en sistemas informáticos realizada de buena fe y con la intención de reportarla.[49] Sin embargo, no es tarea del derecho penal contribuir al desarrollo de actividades sociales, por mucha relevancia que les atribuyan ciertos grupos: antes bien, su función es proteger bienes jurídicos,[50] mediante el castigo de aquellas conductas que los afectan en términos penalmente relevantes. Y, para ello, resulta necesario que el bien jurídico exista como tal, única manera en que podría plantearse su afectación (similar Sternberg-Lieben, 2007: 109). Por ende, la discusión debería centrarse en si el *hacking* (puro o blanco, o ético) lesiona o pone en peligro algún bien jurídico, en el estado en que este se encuentre y no en el estado en que aquel podría llegar a encontrarse gracias al desarrollo de la ciberseguridad.

De otro lado, hacer depender la relevancia penal de la conducta de la intención del hechor, fuera de entrañar una considerable dificultad probatoria, importa condenar la comprensión de la figura al subjetivismo.[51] Frente a ello, una interpretación sustentada en la superación de barreras técnicas confiere (mayor) certeza respecto de cuál era la voluntad del afectado respecto de la información contenida en el sistema y cómo debe entenderse el comportamiento de quien, actuando sin autorización, accede a y conoce (indebidamente) los datos.

Conclusiones

El espionaje informático provoca diversos problemas interpretativos y de delimitación de su injusto. Por un lado, su sentido y alcance no es claro, ni tampoco resulta evidente cómo castigarlo. Por otro lado, el hecho de que vivamos en una sociedad de la información, en la que existe disponibilidad e intercambio permanente de datos, puede generar dificultades al momento de sancionar (penalmente) el acceso a los mismos.

49. En esa línea: Pablo Viollier, «Boletín 12192-25: Delitos informáticos», Derechos Digitales, 3 de enero de 2019, disponible en https://bit.ly/34Kwjva.

50. De ahí que se aluda al principio de exclusiva protección de bienes jurídicos. Por todos, Mir (2016: 129 y ss.).

51. Sobre el problema de las verdaderas intenciones de los *ethical hackers*, véase Jamil y Khan (2011).

El delito de espionaje informático puede impactar negativamente en diversos bienes jurídicos, ya sea individuales o colectivos (por ejemplo, la intimidad o seguridad nacional), lo que a su vez depende de la clase de información con la cual se vincule. Cuando él es ejecutado en el ciberespacio, asume un carácter pluriofensivo, ya que también afecta a la funcionalidad informática, o sea, a aquellas condiciones que posibilitan que los sistemas informáticos realicen en forma adecuada las operaciones de almacenamiento, tratamiento y transferencia de datos, en un marco tolerable de riesgo.

El espionaje informático implica un acceso a y conocimiento indebido de datos. Se trata de un concepto estrechamente relacionado con el de intromisión relativa a datos que no han de ser revelados, pues existen intereses contrarios a que ellos sean conocidos. Esto lo distingue del *hacking* o mero acceso indebido a datos; de la obtención o revelación de datos; así como de los otros delitos que paradigmáticamente integran la criminalidad informática, a saber, el fraude y sabotaje informático.

En tanto recae en información que se espera no trascienda, el espionaje informático tiene puntos de contacto con otros ilícitos de la parte especial, como los delitos contra la intimidad o privacidad; la violación de secretos o la infidelidad en la custodia de documentos; la comunicación fraudulenta de secretos de fábrica o el abuso de información privilegiada; o los delitos contra la propiedad intelectual o industrial. Tratándose de casos en los que se verifica un acceso indebido a datos, tal conexión puede dar lugar a relaciones concursales, sin perjuicio de que el espionaje informático sirva para colmar vacíos de punibilidad existentes en ciertas descripciones típicas.

Para definir el injusto del espionaje informático, resulta clave analizar el concepto de información penalmente relevante. Ella se vincula con intereses de diversa índole e importancia, que pueden verse afectados con distinta intensidad, más allá del riesgo permitido. En este contexto, también ha de considerarse la existencia de barreras técnicas relativas a los datos, pues ellas implican una voluntad inequívoca de exclusión de terceros respecto de su acceso y conocimiento. A su vez, la significancia penal del espionaje, sea en el plano objetivo como subjetivo, debería tenerse en cuenta al consagrar su sanción.

La tipificación del espionaje informático en la Ley 19.223 es fuente de inconvenientes (por ejemplo, en materia de técnica legislativa y aplicación práctica de la figura), que deberían ser revisados en una futura reforma legislativa. En este ámbito, las directrices del CCCE resultan en general más apropiadas y, por lo mismo, cabría considerarlas al momento de (re)tipificar el delito.

Por último, la propuesta de reforma del espionaje informático en actual trámite parlamentario presenta algunos avances respecto de la regulación contenida en la Ley 19.223, en especial en lo que se refiere a la superación de barreras técnicas o medidas tecnológicas de seguridad. Sin embargo, la exigencia de un ánimo especial en la figura del artículo 2 inciso segundo puede limitar la aplicación del delito, sin que se divisen motivos que aconsejen su consagración.

Agradecimientos

Trabajo redactado en el marco del proyecto Fondecyt núm. 1161066: «Los delitos informáticos en el ordenamiento jurídico chileno: Análisis dogmático y crítico, y propuestas de *lege ferenda*». Los autores agradecen asimismo las sugerencias de los árbitros anónimos relativas a la primera versión del presente artículo.

Referencias

Acosta, Juan (1988). «El delito de comunicación fraudulenta de secretos de fábrica (Breve estudio de la figura del art. 284 del C. Penal)». *Revista Chilena de Derecho*, 15: 65-79.

Agustina, José (2009). «La arquitectura digital de internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual». *International E-Journal of Criminal Sciences*, 3: 1-31. Disponible en https://bit.ly/3ppojHF.

Balmaceda, Gustavo (2009). *El delito de estafa informática*. Santiago: Jurídicas de Santiago.

—. (2014). *Manual de derecho penal, parte especial*. Santiago: Librotecnia.

Bermúdez, Jorge y Camilo Mirosevic (2008). «El acceso a la información pública como base para el control social y la protección del patrimonio público». *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 31: 439-468. DOI: 10.4067/S0718-68512008000200012.

Brodowski, Dominik (2019). «Hacking 4.0: Seitenkanalangriffe auf informationstechnische Systeme. Zugleich ein Beitrag zur Theorie und Dogmatik des IT-Strafrechts». *Zeitschrift für Internationale Strafrechtsdogmatik*, 1: 49-61. Disponible en https://bit.ly/34JLDbt.

Corcoy, Mirentxu (2007). «Problemática de la persecución penal de los denominados delitos informáticos: Particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos». *Eguzkilore*, 21: 7-32. Disponible en https://bit.ly/34G503B.

Couso, Jaime (2018). «Relevancia penal de la intromisión del empleador en los correos electrónicos de sus trabajadores». *Revista de Derecho de la Universidad Católica del Norte*, 2: 29-76. DOI: 10.4067/S0718-97532018000200029.

Crovi, Delia (2002). «Sociedad de la información y el conocimiento: Entre optimismo y desesperanza». *Revista Mexicana de Ciencias Políticas y Sociales*, 45 (185): 13-33. DOI: 10.22201/fcpys.2448492xe.2002.185.48317.

Cury, Enrique (2011). *Derecho penal, parte general*. Santiago: Ediciones UC.

Escalona, Eduardo (2004). «El *hacking* no es (ni puede ser) delito». *Revista Chilena de Derecho Informático*, 4: 149-167. DOI: 10.5354/0717-9162.2011.10678.

Etcheberry, Alfredo (2010a). *Derecho penal, parte especial*. Tomo 3. Santiago: Jurídica.

—. (2010b). *Derecho penal, parte especial*. Tomo 4. Santiago: Jurídica de Chile.

Fernández Díaz, Carmen (2018). «La amenaza de las nuevas tecnologías en los negocios: El ciberespionaje empresarial». *Revista de Derecho UNED*, 23: 17-57. DOI: 10.5944/rduned.23.2018.24001.

Flor, Roberto (2012). «Verso una rivalutazione dell'art. 615 *ter* c.p.?». *Diritto Penale Contemporaneo*, 2: 126-142. Disponible en https://bit.ly/38FTrvO.

Flores, Ana, Graciela Galicia y Egbert Sánchez (2007). «Una aproximación a la sociedad de la información y del conocimiento». *Revista Mexicana de Orientación Educativa*, 5 (11): 19-28. Disponible en https://bit.ly/2KBVo4y.

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: 90-107. Disponible en https://bit.ly/3nPLieQ.

García, Gonzalo (2013). «Modelo de protección en normas administrativas y penales que regulan el abuso de información privilegiada en la legislación chilena». *Política Criminal*, 8 (15): 23-63. DOI: 10.4067/S0718-33992013000100002.

García, María (1997). *Falsedades documentales (en el Código Penal de 1995)*. Valencia: Tirant lo Blanch.

García-Pablos, Antonio (2014). *Introducción al derecho penal*. Volumen 1. Madrid: Centro de Estudios Ramón Areces.

García, Gonzalo y Pablo Contreras (2009). «Derecho de acceso a la información en Chile: Nueva regulación e implicancias para el sector de la defensa nacional». *Estudios Constitucionales*, 7 (1): 137-175. DOI: 10.4067/S0718-52002009000100005.

Garrido, Mario (2010). *Derecho penal, parte especial*. Tomo 3. Santiago: Jurídica de Chile.

—. (2011). *Derecho penal, parte especial*. Tomo 4. Santiago: Jurídica de Chile.

Gercke, Marco y Phillip Brunst (2009). *Praxishandbuch Internetstrafrecht*. Stuttgart: Kohlhammer.

Gillespie, Alisdair (2016). *Cybercrime: Key issues and debates*. Londres y Nueva York: Routledge.

Grunewaldt, Andrés (2013). «Delitos contra los derechos de autor en Chile». *Revista Chilena de Derecho y Tecnología*, 2 (2): 95163. DOI: 10.5354/0719-2584.2013.30311.

Gutiérrez, María (1996). «El intrusismo informático (*hacking*): ¿Represión penal autónoma?». *Informática y Derecho*, 12-15: 1163-1184. Disponible en https://bit.ly/3hkLL6n.

Hernández, Héctor (2001). «Tratamiento de la criminalidad informática en el derecho penal chileno: Diagnóstico y propuestas». Informe solicitado por la División Jurídica del Ministerio de Justicia. Inédito.

—. (2020). «Der unbefugte Zugang zu einem Computersystem und die Grenzen des zu beachtenden Willens des Rechtsinhabers». *FS-Sieber* (en prensa): 1-9.

Hilgendorf, Eric y Brian Valerius (2012). *Computer und Internetstrafrecht*. Berlín: Springer.

Holt, Thomas J. (2020). «Computer hacking and the hacker subculture». En *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 725-742). Cham: Palgrave Macmillan, Springer.

Huerta, Marcelo y Claudio Líbano (1996). *Delitos informáticos*. Santiago: Jurídica ConoSur.

Jamil, Danish y Muhammad Numan Ali Khan (2011). «Is ethical hacking ethical?». *International Journal of Engineering Science and Technology*, 3 (5): 3.758-3.763. Disponible en https://bit.ly/2WOtqoO.

Jijena, Renato (1992). *Chile, la protección penal de la intimidad y el delito informático*. Santiago: Jurídica de Chile.

—. (1994). «Debate parlamentario en el ámbito del derecho informático: Análisis de la Ley 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información». *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 15: 347-401. Disponible en https://bit.ly/310CUKW.

Jordan, Tim (2016). «A genealogy of hacking». *Convergence: The International Journal of Research into New Media Technologies*, 23 (5): 528-544. DOI: 10.1177/1354856516640710.

Karagiannopoulos, Vasileios (2018). *Living with hacktivism*. Cham: Palgrave Macmillan, Springer.

Kindhäuser, Urs (1999). «Der Computerbetrug (§ 263a StGB) – ein Betrug?». En *FS-Grünwald* (pp. 285-305). Baden-Baden: Nomos.

Kochheim, Dieter (2015). *Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik*. Múnich: Beck.

Labatut, Gustavo (2012). *Derecho penal*. Tomo 2. Santiago: Jurídica de Chile.

Lara, Juan, Manuel Martínez y Pablo Viollier (2014). «Hacia una regulación de los delitos informáticos basada en la evidencia». *Revista Chilena de Derecho y Tecnología*, 3 (1): 101137. DOI: 10.5354/0719-2584.2014.32222.

Londoño, Fernando (2004). «Los delitos informáticos en el proyecto de reforma en actual trámite parlamentario». *Revista Chilena de Derecho Informático*, 4: pp. 171-190. DOI: 10.5354/0717-9162.2011.10679.

López, Macarena (2002). «Ley 19.223 y su aplicación en los tribunales». En *Derecho y tecnologías de la información* (pp. 397-414). Santiago: Fundación Fueyo, UDP.

Magliona, Claudio (2002). «Análisis de la normativa sobre delincuencia informática en Chile». En *Derecho y tecnologías de la información* (pp. 383-395). Santiago: Fundación Fueyo, UDP.

Magliona, Claudio y Macarena López (1999). *Delincuencia y fraude informático*. Santiago: Jurídica de Chile.

Malamud, Samuel (2018). «Sabotaje informático: ¿La exigencia de daño grave como elemento del injusto?». *Revista Jurídica del Ministerio Público*, 72: 143-161.

Marti, Yohannis y Rosa Vega-Almeida (2005). «Sociedad de la información: Los mecanismos reguladores en el contexto de una sociedad emergente». *Ciência da Informação*, 34 (1): 37-44. DOI: 10.1590/S0100-19652005000100005.

Masís, Jonathan (2016). «El delito de espionaje informático en el derecho internacional y costarricense: Una modalidad de infracción del derecho humano de la intimidad». *Anuario de Derechos Humanos*, 12: 103-118. DOI: 10.5354/0718-2279.2016.42744.

Matus, Jean Pierre y María Cecilia Ramírez (2019). *Manual de derecho penal chileno, parte especial*. Valencia: Tirant lo Blanch.

Mayer, Laura (2017). «El bien jurídico protegido en los delitos informáticos». *Revista Chilena de Derecho*, 44 (1): 235-260. DOI: 10.4067/S0718-34372017000100011.

—. (2018). «Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos». *Ius et Praxis*, 1: 159-206. DOI: 10.4067/S0718-00122018000100159.

Mayer, Laura y Guillermo Oliver (2020). «El delito de fraude informático: Concepto y delimitación». *Revista Chilena de Derecho y Tecnología*, 9 (1): 151-184. DOI: 10.5354/0719-2584.2020.57149.

Medina, Gonzalo (2014). «Estructura típica del delito de intromisión informática». *Revista Chilena de Derecho y Tecnología*, 3 (1): 79-99. DOI: 10.5354/0719-2584.2014.32221.

Mir, Santiago (2016). *Derecho penal, parte general*. Barcelona: Reppertor.

Miró, Fernando (2012). *El cibercrimen.* Madrid: Marcial Pons.

Morón, Esther (2007a). «Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos». En *Delito e informática: algunos aspectos* (pp. 85-128). Bilbao: Universidad de Deusto.

—. (2007b). «Quiebras de la privacidad en escenarios digitales: Espionaje industrial». *Eguzkilore*, 21: 117-144. Disponible en https://bit.ly/34L69IC.

Moscoso, Romina (2014). «La Ley 19.223 en general y el delito de *hacking* en particular». *Revista Chilena de Derecho y Tecnología*, 3 (1): 11-78. DOI: 10.5354/0719-2584.2014.32220.

Muñoz Conde, Francisco (2015). *Derecho penal, parte especial*. Valencia: Tirant lo Blanch.

Oliver, Guillermo (2013). *Delitos contra la propiedad*. Santiago: Legal Publishing.

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*, 41: 211-262. DOI: 10.4067/S0718-68512013000200007.

Perrone, Andrea (2009). «Información en el mercado de valores y tutela del inversor». *Política Criminal*, 4 (7): 197-229. DOI: 10.4067/S0718-33992009000100007.

Picotti, Lorenzo (2013). «Los derechos fundamentales en el uso y abuso de las redes sociales en Italia: aspectos penales (I)». *Revista de Internet, Derecho y Política*, 16: 76-90. Disponible en https://bit.ly/3nSElJN.

Pineda, Migdalia, Esther Durante, Sylvia Fernández y Rocío Belandria (2003). «La sociedad de la información como sociedad en transición: Caracterización, tendencia y paradojas». *Revista de Ciencias Sociales*, 9 (2): 252-270. Disponible en https://bit.ly/2WMojVX.

Rodríguez, José (1956). «Espionaje». En *Nueva enciclopedia jurídica*. Tomo 8 (pp. 791-808). Barcelona: Seix.

Rodríguez, Luis y Magdalena Ossandón (2011). *Delitos contra la función pública*. Santiago: Jurídica de Chile.

Romeo, Carlos (1988). *Poder informático y seguridad jurídica: La función tutelar del derecho penal ante las nuevas tecnologías de la información*. Madrid: Fundesco.

Roxin, Claus (2006). *Strafrecht Allgemeiner Teil*. Tomo 1. Múnich: Beck.

Salvadori, Ivan (2012). «El delito de acceso abusivo a un sistema informático o telemático previsto por el artículo 615-ter del Código Penal italiano». *Perspectiva Penal Actual*, 1: 165-183.

Sestieri, Marcello (2019). «Neutralization theory: Criminological cues for improved deterrence of hacker crimes». *Diritto Penale Contemporaneo*, 2: 1-8. Disponible en https://bit.ly/3aJ6hMp.

Sieber, Ulrich (2014). «§ 24 Computerkriminalität». En *Europäisches Strafrecht* (pp. 435-468). Baden-Baden: Nomos.

Smith, Bryan, William Yurcik y David Doss (2002). «Ethical hacking: The security justification redux». *IEEE*: 374-379. DOI: 10.1109/ISTAS.2002.1013840.

Stern, Enrique (2007). «El sentido de la privacidad, la intimidad y la seguridad en el mundo digital: Ámbitos y límites». *Eguzkilore*, 21: 185-199. Disponible en https://bit.ly/3puT4v3.

Sternberg-Lieben, Detlev (2007). «Bien jurídico, proporcionalidad y libertad del legislador penal». En *La teoría del bien jurídico ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmático?* (pp. 105-127). Madrid-Barcelona: Marcial Pons.

Torres, Cristóbal (2017). «Sociedad de la información y nuevas tecnologías». *Nueva Revista de Política, Cultura y Arte*, 162: 11-20. Disponible en https://bit.ly/38E4dmi.

Velásquez, Fernando (2009). *Derecho penal, parte general*. Tomo 1. Santiago: Jurídica de Chile.

Villacampa, Carolina (1999). *La falsedad documental: Análisis jurídico penal*. Barcelona: Cedecs.

Wells, Fabiana (2020). «Hacked off: How Germany and the United States are dealing with the continuous threat of cyber attacks». *National Security Law Brief*, 10 (1): 343-473.

Winter, Jaime (2013). «Elementos típicos del artículo 2 de la Ley 19.223: Comentario a la SCS de 03.07.2013 rol 923812». *Revista Chilena de Derecho y Ciencias Penales*, 2 (4): 277282.

Sobre los autores

Laura Mayer Lux es abogada. Licenciada en Ciencias Jurídicas por la Pontificia Universidad Católica de Valparaíso, Chile. Doctora en Derecho por la Universidad de Bonn, Alemania. Profesora de Derecho Penal del Departamento de Derecho Penal y Procesal Penal de la Pontificia Universidad Católica de Valparaíso. Su correo electrónico es laura.mayer@pucv.cl. https://orcid.org/0000-0003-1968-6578.

Jaime Vera Vega es abogado. Licenciado en Ciencias Jurídicas por la Pontificia Universidad Católica de Valparaíso, Chile. Doctor en Derecho por la Pontificia Universidad Católica de Valparaíso, Chile. Magíster en Derecho Penal y Ciencias Penales por la Universidad de Barcelona y la Universidad Pompeu Fabra, España. Profesor de Derecho Penal y Procesal Penal del Departamento de Derecho Penal y Procesal Penal de la Pontificia Universidad Católica de Valparaíso. Su correo electrónico es jaime.vera@pucv.cl. https://orcid.org/0000-0002-3748-5182.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).