REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO • UNIVERSIDAD DE CHILE
ISSN 0719-2576 • VOL. 3 NRO. 1 (2014) • PÁGS. 79-99 • DOI 10.5354/0719-2584.2014.32221

Estructura típica del delito de intromisión informática

Defining the crime of illegal access to computer system

GONZALO MEDINA SCHULZ
Universidad de Chile

RESUMEN En Chile, los tribunales han aplicado diferentes criterios para establecer cuándo el acceso a un sistema informático puede ser descrito como no autorizado, interpretación que varía desde la superación de obstáculos técnicos a sólo la contrariedad con la voluntad del titular de los datos, expresada en cláusulas contractuales. Estos diferentes estándares se originan en la estructura usada para sancionar el acceso, la cual no hace referencias ni a la superación de barreras técnicas ni a la voluntad del titular de los datos. Antes de resolver esta discusión, el artículo se refiere brevemente a la situación jurídica en Alemania y España, utilizando esta comparación a fin de destacar algunos de los puntos más discutibles de esta clase de delitos. Finalmente, este trabajo pretende establecer algunos límites a la figura penal bajo la ley chilena.

PALABRAS CLAVE Delitos informáticos, acceso no autorizado, sistema de tratamiento de información, ciberdelito.

ABSTRACT In Chile, courts have applied different criteria to establish when accessing a computer system qualifies as unauthorized, varying the understanding from the circumvention of technical barriers to mere contravening the data owner's will expressed in contractual clauses. These

different standards have their origin in the legal framework that punishes illegal access, which contains reference neither to the data owner's will nor to the circumvention of technical barriers. Before resolving this discussion, this article briefly explains the legal situation in Germany and Spain, using those countries' law for comparison in order to highlight some controversial points of this kind of crimes. Then, this article establishes some limits for illegal access to computer systems under the Chilean criminal law.

KEYWORDS Informatics crimes, non-authorized access, information treatment system, cybercrime.

INTRODUCCIÓN

Los delitos asociados a la informática se han convertido en uno de los temas de mayor desarrollo en el derecho penal de las décadas recientes. Como consecuencia de ello, numerosos países han adaptado su regulación penal, la que en Chile ha permanecido inalterada desde la publicación de la Ley 19.223, que tipifica figuras penales relativas a la informática, el 7 de junio de 1993.

En lo que aquí interesa, la pregunta acerca de la protección de la privacidad de las personas, cuando la información está contenida en un sistema de tratamiento de información, se inserta en el contexto de una regulación penal de la protección de la privacidad que es notablemente asistemática y deficiente en Chile (Medina, 2008: 243-244).

Sin embargo, es posible identificar diversos parámetros en el sistema general de protección de la privacidad que nos llevan a reflexionar acerca de los límites del derecho penal en el ámbito informático. Con ello me refiero a que la privacidad como bien jurídico penal se encuentra sujeto a ciertas restricciones generales en su custodia, dado que se trata de un bien jurídico eminentemente disponible y cuya afectación constante es permanente en las interacciones sociales. Se trata, entonces, de un bien jurídico cuya protección es esencialmente relativa.

En ese sentido, la protección general de las intromisiones físicas en la vida privada de las personas está restringida por el concepto de morada, mientras que las intromisiones por medios de instrumentos —regulado

esencialmente por el artículo 161-A del Código Penal— lo hacen mediante el doble recurso de exigir, por una parte, que se trate de sucesos que ocurran en lugares que no sean de libre acceso al público y de exigir, adicionalmente, que se trate de sucesos de la vida privada, cuestión que no pasa en el caso de los tipos penales informáticos y que tiene consecuencias en la comprensión de lo protegido.

En cuanto a la información protegida y su acceso indebido, nuestra ley penal tiene —además del clásico delito de registro de papeles ajenos—, la protección adicional de la información contenida en soportes informáticos, contenida en la Ley 19.223. Sin embargo, el contexto de tipificación de esta clase de atentados contra la privacidad debe ponderar razonablemente los intereses de los titulares de información, con numerosos supuestos de libre disponibilidad de la misma. En sociedades en las cuales el libre acceso a la información se ha convertido en un bien altamente valioso, resulta indispensable configurar límites razonables a la protección penal informática.

Con todo, como se verá en la revisión de la literatura en el derecho comparado, la afirmación de que la privacidad sea lo protegido en esta clase de delitos no es una cuestión pacífica. Algunos autores ven en esta clase de comportamientos una posible infracción a un derecho de exclusión no necesariamente vinculado con la privacidad, sino más bien específico de la informática.

Sin pretender resolver aquello, este trabajo toma como punto de partida las disposiciones de los artículos 2 y 4 de la Ley 19.223 que protegen esencialmente la privacidad del titular de la información, entendida como la posibilidad de excluir a terceros del acceso a ámbitos de dominio de ese titular. En ese sentido, uno puede compatibilizar esa noción de privacidad con un concepto más formal, no definido por la especial naturaleza (privada) de ciertos sucesos, sino como el reconocimiento de la posibilidad de excluir a terceros como rasgo distintivo.

La pregunta sobre los límites de lo punible depende de dar una serie de respuestas a interrogantes que se pueden plantear en algunos casos. A modo de ejemplo: Juan ingresa a un sitio web en el cual debe suscribir una declaración previa en la que afirma ser residente permanente de la ciudad de Santiago. Sin embargo, él no reside en esa ciudad sino en Valparaíso. Al vulnerar esa condición de ingreso al sitio, ¿comete un ingreso indebido a la información contenida en él? Parece obvia la respuesta ne-

gativa a esa interrogante, pero esa obviedad descansa sobre ciertos parámetros de la configuración del tipo penal, los cuales pueden establecerse al menos en dos formas distintas, lo que se ve reflejado en las diferencias de criterio en los dos fallos que se citan parcialmente a continuación.

El primero es un caso resuelto por la Corte Suprema, que en su primer considerando señala que:

> Que, el hecho establecido en el considerando cuarto del fallo en alzada configura el delito establecido en el artículo 2 de la Ley 19.223, figura penal que protege la privacidad de sistemas informáticos de tratamiento de información sancionando la conducta generalmente denominada «espionaje informático», en la cual incurre el que «con 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», para apreciar el cual resulta conveniente tener presente que el contrato de trabajo del acusado (copia del cual se encuentra a fs. 51) contemplaba en forma especial una cláusula de reserva absoluta respecto de la información contenida en las bases de datos a las que tenía acceso en el desarrollo de las labores propias de su empleo. Asimismo, ha de advertirse que la conducta del procesado se verificó en circunstancias que terminaba de prestar servicios para la querellante, para incorporarse a otra empresa de la competencia, apropiándose de la base de datos confidencial de propiedad de la querellante, consistente en el archivo computacional que contenía el listado general de su empleadora, así como el archivo con el listado de números telefónicos del sistema de discado rápido de ésta, todo lo cual lo envió vía *e-mail* a la cuenta personal de su cónyuge, a su propio domicilio, procediendo a continuación a incorporarla a su propio computador, traspasando la información a su agenda personal. De otra parte cabe tener presente que, conforme declaran R. C. a fs. 12 vta., jefe de exportaciones de la querellante y E. M. a fs. 108, gerente de ventas de la empresa A. P. L., nueva empleadora del procesado, en el desempeño de sus nuevas funciones para esta última, utilizó la información de la que Z se había apropiado, contactando a clientes de la cartera de la Compañía Y.[1]

Un caso aparentemente similar es el resuelto por el Cuarto Tribunal de Juicio Oral en lo Penal, que en su considerando decimoctavo señala:

1. Corte Suprema, 30 de julio de 2008, rol 14526-2005.

Calificación jurídica: Que el delito contemplado en el artículo 2 de la Ley 19.223 dice «el que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio».

En este caso, el sujeto accedió y conoció indebidamente la información contenida en un sistema de tratamiento de la misma; delito que en concepto de estos sentenciadores se encuentra acreditado, toda vez, el acusado G. R. T., mediante un estudio del sistema de ingreso al portal de comercio electrónico denominado «Chilecompra», logró ingresar en forma reiterada y automatizada, mediante un mecanismo que permitió la suplantación de la calidad de «comprador» accediendo directamente a conocer el cuadro comparativo de cientos de miles de ofertas cerradas y decenas de ofertas abiertas en estado de publicadas, de muy distintos rubros, circunstancias prohibidas por las condiciones de uso del portal, políticas aceptadas previamente al registrarse como usuario lícito en el sistema.

El acceso indebido no dice relación como lo ha sostenido la defensa con el hecho que acceda al portal con su *password* de usuario. El acceso indebido es aquel que realiza para llegar a la página reservada, violando las barreras impuestas por el sistema con el ánimo de conocer la información secreta. G. R. T. obtuvo una información en forma no autorizada, sea cual sea su motivación.

En este caso, la conducta desplegada por el acusado G. R. T. fue más allá de un simple acceso indebido o *hacking* directo, por cuanto la reiteración de éstos, por un periodo prolongado de tiempo, desde su IP y respecto de licitaciones que no dicen relación con el rubro farmacéutico, permitió concluir que los ingresos indebidos tuvieron como objetivo conocer la información contenida en la plataforma comercial virtual de Chilecompra.

Cabe precisar que el Tribunal tiene claro que sólo 21 de los accesos indebidos se realizaron manualmente por G. R. T. y que el resto de los 333.000 y tantos ingresos se hizo con un *software* creado por él y manipulado respecto de estos ingresos desde las IP ubicadas en su dirección registrada en la GTSD de Internet, la empresa es MXXX pero él es su representante legal y creador del software.

Y por último, no cabe duda que la plataforma comercial electrónica de Chilecompra es un sistema de tratamiento de la información, habiéndose acreditado latamente el secreto de las licitaciones en estado de publicar, que obviamente constituye información privilegiada.[2]

2. Cuarto Tribunal Oral en la Penal, 2 de septiembre de 2009, RIT 135-2009.

Los casos anteriores permiten ilustrar la cuestión relevante en la protección de la privacidad en el contexto de sistemas informáticos y es que el concepto de lo «indebido» en el acceso a la información es conflictivo en cuanto al establecimiento de sus límites. Si uno observa ambas sentencias, la primera toma en consideración las obligaciones contenidas en el contrato de trabajo para determinar lo indebido del acceso, mientras la segunda se concentra más en las cuestiones referidas a la superación de las barreras informáticas que impiden el acceso de cualquiera a la información contenida en un sistema informático.

Mi intención en lo que sigue es explorar brevemente el alcance de una u otra opción interpretativa de las disposiciones de la Ley 19.223 y determinar cuál, en mi opinión, debiera ser la manera correcta de dotar de contenido a la figura penal, centrándome no en la discusión sobre el bien jurídico protegido, sino más bien en el núcleo típico del injusto, a fin de obtener una interpretación que tenga ciertos rendimientos restrictivos del alcance de la disposición.

EL ARTÍCULO 2 DE LA LEY 19.223 FRENTE AL DERECHO COMPARADO

El artículo 2 de la Ley 19.223[3] sanciona una serie de conductas con diversos componentes que permiten establecer la relevancia penal de un comportamiento. En esta ocasión, me interesa analizar una modalidad específica: el acceso a un sistema de tratamiento de la información con el ánimo de conocer indebidamente la información contenida en él.

Esta modalidad en particular resulta ser especialmente importante en la actualidad, dado que existen diversas clases de información con relevancia para terceros, sobre todo cuando pueda tener algún valor patrimonial.

Una lectura de la disposición penal vigente en Chile que considere como indebido todo acceso contrario a la voluntad del titular de la información, nos conduce inevitablemente a una discusión sobre la amplitud de la protección penal frente a esta clase de comportamientos. Los términos de tal discusión dependen de la forma en la cual se establezca

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

la protección de la privacidad en nuestro sistema penal y se dote de contenido a la modalidad de acceso y al requerimiento de un ánimo de usar, conocer o apoderarse indebidamente de la información.

EL TIPO PENAL ALEMÁN

Es correcto afirmar que la redacción de nuestro tipo penal no es idéntica a la fórmula usada por el derecho alemán, el cual expresamente establece, en la sección 202a *Strafgesetzbuch* (StGB),[4] que la punibilidad de la conducta está dada por la superación de medidas de seguridad de acceso a la información y que la misma está especialmente protegida contra el acceso indebido.[5]

La doctrina alemana afirma que la disposición se orienta a la protección del secreto de datos formal (*formelles Datengeheimnis*) (Graf, 2012: 2), el poder de disposición formal (Kargl, 2013: 3) o bien ambos junto con la privacidad (Kühl, 2011: 1).

En consonancia con el objeto de protección, el tipo penal alemán exige que los datos objeto del delito no estén destinados al autor de la conducta, lo cual se determina de acuerdo a la voluntad del titular de los mismos (Graf, 2012: 19), quien puede disponer, respecto de terceros, de condiciones de acceso o uso de los datos, las que puede ser limitadas en el tiempo o sujetas a cualquier otra condición (Graf 2012; 20; Kargl, 2013: 8).

La expresión de la titularidad de los datos suele expresarse con mecanismos de exclusión del libre acceso de terceros, como por ejemplo con contraseñas propias en los sistemas utilizados en el lugar de trabajo (Kargl, 2013: 7), sin perjuicio de que no debe confundirse la destinación de los datos a un sujeto determinado con la existencia de medidas de seguridad, como en una prueba de funcionamiento de medidas de seguridad de un sistema, caso en el cual los datos están protegidos contra el

4. Código Penal alemán (N. del E.).

5. «§ 202a. Espionaje de datos. 1) Quien sin autorización se procure para sí o para otro acceso a datos que no estén destinados a él y que estén especialmente asegurados contra su acceso no autorizado, por medio de la superación de la protección de acceso, será castigado con pena privativa de libertad de hasta tres años o con multa. 2) Datos en el sentido del inciso 1, son sólo aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible.» La traducción es nuestra.

acceso, pero sí están destinados a quien tiene por función acceder a los mismos (Dietrich, 2009: 88). También podría ser el caso de los datos protegidos contra accesos no autorizados cuando un tribunal encomienda a funcionarios policiales acceder a los mismos.

El siguiente elemento se refiere a las condiciones técnicas de protección de la información, pues el tipo penal exige que el acceso se realice respecto de datos especialmente protegidos contra accesos no autorizados. Al respecto, se ha afirmado que se trata de la expresión del titular de los datos de mantener la confidencialidad de los mismos (Graf, 2012: 32), en la medida que impida o dificulte el acceso a ellos (Kühl, 2011: 4).

En cuanto al componente de «no autorizados» se indica que se refiere a la idea de que el sujeto que accede a los datos no es un destinatario de los mismos (Graf 2012: 34), reafirmado el primer elemento de la disposición (Kargl, 2013: 11), por lo que se trata de la expresión de un elemento general de antijuridicidad (Lenckner y Eisele, 2010: 11).

Respecto a la exigencia de superación de mecanismos técnicos de protección, se trata de un requisito que apunta a la entidad de la conducta criminal y que excluye la protección frente a conductas negligentes del titular de datos (Kargl, 2013: 14). Dichos mecanismos no pueden consistir en meras medidas organizativas o autorizaciones de acceso (Graf, 2012: 35), sino que pese a la diversidad de mecanismos, el más habitual es el uso de contraseñas (Graf, 2012: 42). Relevante es que la superación de mecanismos técnicos sea causal respecto al acceso a los datos contenidos en el sistema (Lenckner y Eisele, 2010: 10a).

Una pregunta especial que se plantea es el caso del administrador de un sistema de tratamiento de información, respecto del cual deberíamos tener algunas consideraciones adicionales. La función del administrador implica habitualmente la inexistencia de medidas especiales de resguardo para el acceso a los datos contenidos en el sistema. Sin embargo, su acceso está habitualmente vinculado a las funciones de administración del sistema, que se limitan a la actualización de *software*, mantenimiento del acceso a la red o la solución de problemas de funcionamiento. Por ello, los datos contenidos en el sistema, como por ejemplo el tráfico de correo electrónico, no están destinados a su acceso. De esa forma, una utilización no autorizada del acceso del administrador puede constituir una forma de evitar las medidas de seguridad habituales y con ello configurar el tipo penal (Graf, 2012: 43).

EL TIPO PENAL ESPAÑOL

El artículo 197 del Código Penal español[6] trata de diversas modalidades de conducta típica, el apoderamiento de correos electrónicos en el numeral 1 y el apoderamiento de datos reservados de carácter personal o familiar que se encuentren registrados en ficheros o soportes informáticos, electrónicos o telemáticos, en el numeral 2. Pero la modalidad típica que nos interesa es la del numeral 3, que castiga el acceso a datos contenidos en un sistema informático actuando sin autorización y vulnerando las medidas de seguridad dispuestas para impedir el acceso.

Esta última variante fue introducida el año 2010 por el legislador español y se ha afirmado respecto a ella que se trataría no de la protección de la intimidad, sino más bien de la seguridad de los sistemas informáticos como un bien jurídico instrumental (Tomás-Valiente, 2010: 803) o bien del poder de exclusión de terceros frente a sus datos, independiente del contenido reservado de los mismos e indirectamente de la seguridad informática (Salvadori, 2012: 37), o de los que algunos denominan

6. Artículo 197. 1) El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2) Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. 3) El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

indemnidad o integridad del sistema informático (Fernández Teruelo, 2011: 197).

Más allá del evidente requisito de la falta de autorización, la norma española exige la vulneración de barreras de seguridad, las cuales pueden ser tanto físicas como informáticas, tales como claves, huellas dactilares u otros mecanismos similares (Salvadori, 2012: 35). Lo relevante de esa exigencia está dado precisamente para la afirmación de que lo efectivamente protegido es la intimidad. A diferencia de los numerales previos, no se exige una naturaleza especial de los datos, esto es, que sean secretos o reservados, pues basta con la existencia de la barrera de ingreso al sistema, con lo cual se puede reconducir la protección a la idea de privacidad (Matellanes Rodríguez, 2009: 63).

Particularmente interesante resulta la sanción de la permanencia antijurídica en el sistema informático, con lo cual la figura alcanza cierto paralelo con la moderna formulación del allanamiento de morada, que no sólo sanciona el ingreso indebido a un recinto, sino también la permanencia en el recinto contra la voluntad del titular, cuestión que en Chile no se presenta en la regulación del allanamiento de morada (Medina, 2008: 251).

CONCLUSIONES PRELIMINARES

Al mirar brevemente las disposiciones pertinentes de los dos ordenamientos jurídicos, parecen surgir rasgos comunes en la forma en la cual se estructura la protección penal frente a intromisiones informáticas. Tanto la exigencia de contrariedad de voluntad del titular de la información, así como la exigencia de superación de barreras técnicas, son elementos incorporados por esos tipos penales.

En igual sentido, el trabajo dogmático que se ha hecho sobre estas disposiciones penales da cuenta de algunas de las complejidades que una regulación adecuada de estos comportamientos debe enfrentar. Por ello, han de tomarse en consideración esos aspectos al momento de revisar la regulación nacional y los problemas de alcance de la norma chilena.

De esta simple revisión de la regulación alemana y española es posible desde ya advertir numerosas diferencias con la legislación vigente actualmente en Chile. En primer lugar, la estructura de las disposiciones penales pertenecientes a otros ordenamientos jurídicos reconoce de ma-

nera nítida la estructura de un delito contra un ámbito de exclusión de terceros. Más allá de adoptar la idea de la protección de una esfera formal de datos protegidos en un sistema, se trata siempre de una forma de afectación de una legítima pretensión de exclusión de terceros al acceso a un determinado contenido informativo.

Debe tenerse en consideración que no se trata de datos cualificados por una condición especial que los califique como privados o reservados en algún sentido, sino que, en esto coincide con las demás regulaciones, sólo debe tratarse de ciertos datos no disponibles para terceros.

Si se sigue esa idea, parece necesario que el contenido del injusto deba estar configurado por una cierta forma de expresión de la pretensión de excluir a terceros de un ámbito en el cual el titular del mismo puede ejercer exclusión. En el caso alemán y en el español ello se expresa en la exigencia de que la información esté dotada de medidas de protección contra el acceso de terceros y que el acceso a los mismos se produzca por medio de la superación antijurídica de esas barreras técnicas.

Ello parece razonable y obliga a revisar la opinión existente sobre la mayor amplitud de la protección otorgada bajo la ley chilena, además de permitir una revisión crítica de los criterios expresados por nuestra jurisprudencia para dar por establecida la punibilidad de una conducta determinada.

EL TIPO PENAL EN LA LEY CHILENA

La disposición chilena se refiere al acceso a un sistema de tratamiento de la información con ánimo de conocer indebidamente la información contenida en él. Como puede apreciarse, existen diversas diferencias con las dos tipificaciones del derecho comparado que se han tenido a la vista.

Dos diferencias resaltan en cualquier comparación, la primera referida a la inexistencia de alguna referencia a la contradicción con la voluntad del titular de los datos y, la segunda, que se expresa en la ausencia de algún requisito que nítidamente se refiera a mecanismos especiales de vulneración de medidas de seguridad.

Con ello en mente, es claro por qué tradicionalmente se ha afirmado que nuestro derecho protege los sistemas de tratamiento de información de manera más amplia que otras legislaciones, en las cuales se requiere que la información contenida en el sistema de tratamiento de la misma

esté especialmente protegida contra el acceso no autorizado (Magliona Markovicth y López Medel, 1999: 167). Si se sigue esa interpretación, entonces deberíamos afirmar sin mayor dificultad que ambas sentencias citadas al comienzo de este trabajo estarían correctamente fundadas, pues la idea de acceso indebido se da en ambos casos.

Con todo, debe tenerse en consideración que el tipo penal chileno está estructurado sobre la base de la protección de toda clase de contenidos de un sistema de tratamiento de información, pues no exige de ellos alguna cualidad especial, en particular, de que se trate o no de información privada o reservada.

Ello parece ser indicativo de que la protección dispensada no está orientada a la idea de privacidad únicamente, sino que podría asimilarse más bien a la forma de comprensión del objeto de tutela que la literatura alemana sostiene respecto de la correspondiente disposición penal.

Éste no es un punto que pretendo agotar en este trabajo, y que se refiere más bien a si la estructura del tipo penal chileno se trata de un delito de lesión contra la privacidad, como puede ser leído entre nosotros el delito del artículo 161-A del Código Penal, o es más bien una especie de puesta en peligro abstracta, en la forma en que en nuestro ordenamiento jurídico opera el delito de allanamiento de morada. Sin embargo, las conclusiones que aquí se formulan respecto a la estructura típica siguen siendo igualmente válidas en ambas variantes

A continuación se examinan los dos principales elementos del delito, referidos a lo que entendemos por acceso a un sistema y cuándo podemos juzgar a ese acceso como uno de carácter ilícito en términos penales. Adicionalmente, se expondrán a continuación otros criterios de restricción del alcance de la figura delictiva, indispensables para asegurar una correcta comprensión del tipo penal.

ACCESO AL SISTEMA

Por acceso a un sistema de tratamiento de información se ha entendido el penetrar o ingresar a un sistema de tratamiento de la información, permaneciendo en él o no (Magliona Markovicth y López Medel, 1999: 167).

En cuanto al acceso, este elemento debería interpretarse en el sentido de considerar que su formulación da cuenta de la idea de un espacio cerrado, físico o virtual, al cual un sujeto determinado ingresa. El in-

greso es en todo caso a los datos contenidos en el respectivo sistema de tratamiento de información. Sin embargo, no parece que el tenor de la disposición permita extender la figura a uno de los supuestos posibles, referido a la permanencia en el sistema una vez que se ha tenido un acceso autorizado.

La discusión respecto a ese caso pasa necesariamente por dotar de contenidos más precisos a la idea de acceder. Así, si una persona es autorizada para acceder a los datos contenidos en un sistema informático, la autorización para estar en el sistema puede estar limitada tanto temporalmente como en cuanto a los datos del sistema a los cuales pueda acceder.

Por ello, el acceso a un sistema no tiene que considerarse siempre incondicionado. Si uno hace un paralelo con el delito de allanamiento de morada, cuestión que ha sido tomada en consideración en algunos ordenamientos jurídicos (Winn, 2007: 1398), el acceso a alguna dependencia de un hogar no necesariamente implica que el titular de la morada permite el acceso a cualquier dependencia.

En los mismos términos anteriores, el acceso a ciertos datos de un sistema de información no autoriza el conocimiento de los restantes datos contenidos en él, siempre y cuando uno pueda afirmar que los restantes datos se encuentran de alguna manera protegidos contra el acceso, con lo cual, uno debiese afirmar que en los casos en que se accede a un determinado sistema que contiene informaciones diversas de forma fragmentada, cada una de las entradas puede ser un acceso, juzgable como debido o indebido. Lo anterior sin perjuicio de entender la posibilidad de juzgar el acceso a distintas carpetas de un mismo sistema como una forma de unidad de acción.

LO INDEBIDO DEL ACCESO

La norma exige que el acceso se realice con el ánimo de conocer indebidamente del contenido de la información. Sin perjuicio de que a primera vista parece natural desprender que se trata meramente de una exigencia de tendencia interna trascedente que va más allá del mero dolo de acceder, esta interpretación meramente subjetiva es en mi opinión insuficiente para construir el injusto penal. El problema esencial no es uno subjetivo, como algún sector de la literatura lo ha afirmado (Escalona, 2004: 152), sino uno referido a la tipicidad objetiva de la conducta.

En efecto, para que se construya la vulneración de la privacidad por parte de quien accede, es preciso establecer que dicho acceso a la información que se pretende conocer no sólo es dolosa, sino que sin autorización del titular de la información, esto es, sin derecho. Sólo en la medida que se establezca esa contrariedad al ordenamiento jurídico, el tipo penal pude alcanzar límites razonables de aplicación. De esa forma, no se trata sólo de una cuestión relativa a la intención del agente, sino que precede a esa intención particular el hecho de que el autor no tiene derecho a conocer la información contenida en el sistema de tratamiento de la información. Esta manera de leer la disposición penal acerca por cierto el tipo chileno a las disposiciones del derecho comparado, pero la necesidad de dotar a la norma de ese contenido está dada por la estructura propia de la afectación de la privacidad como un derecho a excluir a terceros del acceso a ciertos contenidos que el titular se reserva para sí.

Al tratarse de un bien, o derecho, eminentemente disponible y cuya utilidad social desaparece sin esa disponibilidad, sólo el complemento del injusto dota de sentido a la prohibición. Esto es especialmente relevante cuando se trata de información contenida en sistemas informáticos, los cuales pueden estar naturalmente sujetos a accesos por parte de múltiples personas.

Por lo tanto, el acceso con ánimo de conocer indebidamente del contenido de la información se refiere, en primer término, al conocimiento por parte del autor de que se obra fuera de los límites que el titular de la información ha establecido para acceder a ello.

Con todo, esa interpretación de la idea de lo indebido aun requiere de un complemento, pues la mera contrariedad a la voluntad del titular de la información resulta ser incluso un criterio insuficiente para resolver cuestiones relativas a la relevancia penal de un comportamiento, siendo ello un criterio en principio quizá relevante para otras áreas del derecho, como el laboral o administrativo por ejemplo, pero, como se demuestra más adelante, la mera contrariedad a voluntad no da cuenta suficientemente del problema penal.

RESTRICCIONES ADICIONALES AL CAMPO DE APLICACIÓN

Establecido que el acceso indebido, debe ser interpretado como una exigencia de que el acceso sea sin autorización del titular de la información

contenida, lo cual resulta en principio compatible con ambos fallos citados al comienzo de este trabajo. Queda aún por resolver si la entidad del tipo penal se satisface únicamente con cualquier contradicción con la voluntad del titular de la información o se requiere una forma cualificada de acceso a los mismos.

Ahora llegamos al problema determinante, que se relaciona con el alcance de la prohibición. Imaginemos el siguiente caso: un Juez de Garantía que tiene acceso a las bases de datos del Registro Civil que contiene los antecedentes penales de condenados. Sin duda ese acceso es relevante para el correcto desarrollo de la función del Juez. Sin embargo, el Juez, quien es dueño de una propiedad inmueble que desea poner en arriendo, decide mirar si los posibles arrendatarios han sido o no condenados penalmente.

Una primera lectura podría llevarnos a afirmar que el Juez que ingresa a la base de datos del Registro Civil para buscar esa información accede con el ánimo de conocer indebidamente información contenida en el sistema de tratamiento de la misma. Existen dos posibles respuestas frente a esa interrogante: que se trata de un delito del artículo 2 de la Ley 19.223 y de una infracción administrativa o que sólo se trata de una infracción administrativa, pero que no alcanza la entidad de la conducta penal.

La distinción esencial está dada por la manera en que un titular de información contenida en un sistema puede excluir a terceros de la misma. Ello puede llevarse a cabo por métodos basados en códigos o por vía contractual (Kerr, 2003: 1644). En el caso de trabajadores o funcionarios que acceden a los datos de manera no conforme con la finalidad para la cual se les ha dado acceso, bajo la doctrina alemana esto no es constitutivo de delito pues los datos siguen estando destinados a esas personas (Graf, 2012: 21).

Una pura restricción en base a términos convencionales de uso parece no ser la respuesta adecuada al problema de la determinación de lo indebido de un acceso, si uno lo ve desde la perspectiva de la legítima expectativa de privacidad que puede tener el titular de los datos (Winn, 2007: 1431).

En los casos de superación de regulación con base a códigos, para superarlos el agente debe «engañar» al sistema que contiene la información, aparentando ser un usuario con mayores privilegios (Kerr, 2003:

1.645-1.646) o bien explotando una falencia en el sistema de manera de obtener más acceso que el debido (Kerr, 2003: 1646), lo cual puede justificar en opinión de algunos el reproche penal por la expresión de una mayor peligrosidad del autor por esta particular forma de realización de la conducta, el burlar barreras técnicas (Dietrich, 2009: 387).

En cambio, la protección por medio contractual sólo implica una falta de cumplimiento de los términos de uso del sistema, como en los casos en los cuales un sitio web determinado exige ciertas declaraciones por parte del usuario que accede al sitio (Kerr, 2003: 1646), aunque no pueda afirmarse claramente que, por el contrario, una restricción en base a códigos es una manifestación de voluntad de exclusión por parte del titular de la información, pues éste habitualmente no dispone de alternativas en cuanto a exigir o no, por ejemplo, una identificación por medio de clave (Dietrich, 2009: 236).

Con todo, la mera superación de barreras técnicas no debería considerarse sin más una forma de acceso indebido, como puede apreciarse en el siguiente caso: un titular de una cuenta bancaria intenta acceder a ella, pero ha olvidado su clave. A fin de poder acceder, ingresa al azar algunas claves, hasta que una de ellas resulta correcta. Puede tratarse de una violación a los términos de uso del sitio web de la institución bancaria y aun uno podría afirmar el uso de un método de superación de una barrera de acceso en base a códigos, pero difícilmente se puede afirmar que se trata de un acceso indebido (Winn, 2007: 1432).

Restringir el acceso indebido a los casos de afectación sólo de restricciones en base a códigos permite compatibilizar el interés del libre acceso a información y a la libertad en Internet con la debida protección de la seguridad y privacidad de las personas (Kerr, 2003: 1649) y, en cierto sentido, introduce al mismo tiempo cierto orden de consideraciones víctimo-dogmáticas, en términos de la autoprotección de la víctima respecto a la protección de su privacidad, cuestión que ha sido recogida entre nosotros (Winter, 2013: 272-282).

En el mismo orden de ideas, permite también generar certezas para todos los involucrados en cuanto a la expresión de la pretensión de exclusión de terceros respecto de ciertos ámbitos de información, lo cual es más compatible con la amplitud de la disposición, que no exige un carácter secreto o reservado de la información a la cual se accede, interpretación que resulta coherente con las exigencias que he planteado para

el tipo penal de registro de papeles ajenos del artículo 146 del Código Penal, al exigir también ciertos mecanismos de resguardo de los papeles objeto del delito (Medina, 2008: 252).

Si la barrera para terceros no está dada por la clase de información protegida, entonces sólo queda como criterio razonable el de la expresión de una voluntad de exclusión de terceros, que no se extienda a la posible arbitrariedad de la mera afirmación contractual de no permitir un acceso a terceros.

En términos de la asimilación del estatuto del allanamiento de morada en comparación con el acceso indebido a sistemas informáticos, no se puede equiparar el cerrar la puerta de una casa y la reja externa, a dejar todo abierto y colocar un letrero que diga «no entren extraños» (Kerr, 2003: 1646).

EL PROYECTO DE CÓDIGO PENAL 2014

El proyecto de Código Penal de 2014[7] contempla modificaciones significativas en comparación con la regulación actualmente vigente. Sin perjuicio de que no trae un apartado especialmente dedicado a una categoría de delitos informáticos, en el contexto genérico de la protección de la privacidad se encuentra una disposición del siguiente tenor:

> Artículo 275. Intromisión. Será sancionado con la pena de multa, reclusión o prisión de 1 a 3 años, el que sin el consentimiento del afectado y usando dispositivos técnicos captare:
>
> 1.° la imagen o el sonido que tiene lugar dentro de la morada de otro;
>
> 2.° la comunicación que dos o más personas mantienen privadamente;
>
> 3.° la imagen de una acción o situación respecto de la cual el afectado tiene una expectativa legítima de intimidad, manifestada en las circunstancias en que ocurre dicha acción o situación.
>
> Con la misma pena será sancionado el que sin el consentimiento del afectado accediere a la información que otro tuviere en cualquier soporte o medio que cuente con mecanismos de resguardo que impidan el libre acceso a ella, vulnerándolos.

El inciso final establece una restricción coherente con la interpretación aquí propuesta del tipo penal actualmente contemplado en nuestro

7. Boletín 9274-07, del 10 de marzo de 2014, que establece un nuevo código penal.

ordenamiento jurídico. Así, existe tanto la referencia a la contrariedad a la voluntad del titular de la información, pero exige adicionalmente la vulneración de mecanismos de resguardo que custodian la información.

Sin duda la interpretación de esos mecanismos de resguardo no debería orientarse a una interpretación en sentido amplio, entendiendo por tales no sólo las restricciones con base en código sino también las contractuales, pues de esa forma se pierde toda la intención de expresar una cierta relevancia de los criterios de restricción de la punibilidad.

En ese mismo sentido debería entenderse la disposición final que exige la vulneración de los mecanismos de resguardo. Una lectura correcta de la propuesta legislativa debería ser plenamente compatible con las exigencias típicas demandadas en este trabajo, además de armonizarse con las formulaciones empleadas en otros sistemas jurídicos.

Adicionalmente, es acertado en mi opinión que se trate de una regulación conjunta de la afectación de la privacidad, con independencia de los medios. Que éstos sean o no informáticos no debería ser el criterio determinante de la sistemática de la regulación penal, sino que una regulación conjunta de los medios de intromisión da cuenta de que no se trata de bienes jurídicos nuevos derivados del impacto de la informática, sino de la protección de bienes jurídicos clásicos, frente a nuevas formas de afectación.

A MODO DE CONCLUSIÓN

Sin duda el uso de sistemas de tratamiento automatizado de información ha tenido una espiral creciente en nuestras sociedades y es previsible que ese uso no decrezca sino que, por el contrario, aumente en el futuro.

Con ello en mente, es indispensable desarrollar una labor dogmática que permita conciliar las ventajas y los riesgos que los usos de la informática presentan. El intento de este trabajo es sentar algunas bases para una discusión sobre los límites apropiados de la protección penal, que no conviertan acciones cotidianas en posibles infracciones penales.

El acceso ilícito a sistemas informáticos es una conducta que ha dejado de ser una cuestión particular de la informática, pues en la medida que ésta determina la manera en la cual operamos en la mayoría de los aspectos de nuestra vida, dicha clase de comportamiento alcanza connotación en la vida social y económica de las personas.

Como revelan los casos citados al inicio de este trabajo, los límites sobre el acceso a información relevante tienen efectos en cuestiones tan diversas como la gestión del Estado o el marco de las relaciones laborales. Por ello, se torna imprescindible profundizar en los alcances que las figuras penales informáticas tienen en estos ámbitos.

Sin duda, requerir la superación de barreras técnicas como un elemento de lo indebido del acceso permite dar más seguridad respecto de las posibles infracciones penales, así como objetivizar los baremos según los cuales atribuimos responsabilidad penal. En mi opinión, existen buenos argumentos para desechar la mera infracción de términos contractuales como criterio suficiente para dotar de reproche penal a un comportamiento. De lo contrario, la sola contrariedad a la voluntad del titular sería criterio suficiente de sanción penal, con las indeseables consecuencias ya expuestas.

No se trata de intentar acercar la disposición chilena a las de otros países sin base alguna, sino que la exigencia de superación de barreras técnicas es una forma razonable de constatar una pretensión nítida de la exclusión de terceros de la información contenida en el sistema, así como a su vez exigir la superación de esas barreras da cuenta de una forma de comportamiento que puede fundar un reproche penal más compatible con la sistemática de la protección de la privacidad en términos penales.

Con todo, es deseable una reforma legislativa que establezca de manera nítida esta clase de exigencias, de modo similar a las legislaciones citadas. La propuesta aquí formulada, por medio de la revisión de los parámetros del derecho comparado, así como mediante una visión sistemática de los distintos delitos en juego y de la comprensión correcta de los elementos de la norma, pretende aportar algunos criterios que permitan operativizar el juicio de merecimiento de reproche penal.

Sin duda, es mucho lo que resta por revisar, en especial cuáles son las implicancias que resultan de los criterios propuestos, para la interpretación de las restantes modalidades típicas de la misma disposición penal, lo que por cierto puede contribuir a delimitar de mejor manera los alcances de todo el tipo penal.

Sin perjuicio de lo anterior, una labor dogmática en este sentido pretende contribuir tanto a una lectura más correcta de las disposiciones vigentes, así como un insumo a las futuras y necesarias reformas legislativas en una materia de regulación dinámicamente cambiante.

REFERENCIAS

Dietrich, Ralf (2009). *Das Erfordernis der besonderen Sicherung im StGB am Beispiel des Ausspähens von Daten, § 202a StGB. Kritik und spezialpräventiver Ansatz*. Berlín: Duncker & Humblot.

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

Fernández Teruelo, Javier Gustavo (2011). *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*. Valladolid: Lex Nova.

Graf, Jürgen-Peter (2012). «Kommentar zur §202a StGB«. En Joecks, Wolfgang y Klaus Miebach (editores), *Münchener Kommentar zum Strafgesetzbuch*, Band 3. Munich: C.H. Beck.

Kargl, Walter (2013). «Kommentar zur §202a StGB». En Kindhäuser, Urs, Ulfrid Neumann y Hans-Ullrich Paeffgen (editores), *Nomos Kommentar zum Strafgesetzbuch*, Band 4. Baden-Baden: Nomos.

Kerr, Ori (Cybercrime's Scope) (2003). «Interpreting 'access' and 'authorization' in computer misuse statutes». *NYU Law Review*, 78 (5): 1.596-1.668.

Kühl, Kristian (2011). «Kommentar zur §202a StGB». En Lackner, Karl y Kristian Kühl (editores), *Strafgesetzbuch Kommentar*, 27. Munich: C.H.Beck.

Lenckner, Theodor y Jörg Eisele (2010). «Kommentar zur §202a StGB». En Schönke, Adolf y Horst Schröder (editores), *Strafgesetzbuch Kommentar*, 28. Munich: C.H. Beck.

Magliona Markovicth, Claudio y Macarena López Medel (1999). *Delincuencia y fraude informático: Derecho comparado y Ley* 19.223. Santiago: Jurídica.

Matellanes Rodríguez, Nuria (2009). «Vías para la tipificación del acceso ilegal a los sistemas informáticos (y II)», *Revista Penal*, 23: 52-72.

Medina, Gonzalo (2008). «Algunos aspectos de la protección penal de la privacidad». En José Ángel Fernández Cruz (coord.), *Estudios de ciencias penales. Hacia una racionalización del derecho penal. IV Jornadas Nacionales de Derecho Penal y Ciencias Penales* (pp. 241-262). Valdivia: Legal Publishing.

Salvadori, Iván (2012). «Los nuevos delitos informáticos introducidos

en el Código Penal Español con la Ley Orgánica 5/2010». En Fernando Pérez Álvarez (editor), *Delito, pena, política criminal y tecnologías de la información y la comunicación en las modernas ciencias penales: Memorias II Congreso Internacional de Jóvenes Investigadores en Ciencias Penales* (pp. 29-50). Salamanca: Ediciones Universidad de Salamanca.

Tomás-Valiente, Carmen (2010). «Del descubrimiento y revelación de secretos». En Manuel Gómez Tomillo y otros, *Comentarios al Código Penal*. Valladolid: Lex Nova.

Winn, Peter A. (2007). «The guilty eye: Unauthorized access, trespass and privacy». *The Business Lawyer*, 62: 1.395-1.437.

Winter, Jaime (2013). «Elementos típicos del artículo 2 de la Ley 19.223: Comentario a la SCS de 03.07.2013, rol 9238-23». *Revista Chilena de Derecho y Ciencias Penales*, 4: 277-282.

SOBRE EL AUTOR

Gonzalo Medina Schulz es abogado. Licenciado en Ciencias Jurídicas y Sociales por la Universidad de Chile. Profesor Asistente del Departamento de Ciencias Penales de la Facultad de Derecho de la Universidad de Chile. Su correo electrónico es <gmedina@gmx.de>. Una primera versión de este artículo fue presentada como ponencia en el Seminario sobre Delitos Informáticos celebrado los días 5 y 6 de noviembre de 2013 en la Universidad de Chile, y organizado por el Centro de Estudios en Derecho Informático de dicha casa de estudios en conjunto con la ONG Derechos Digitales, con el apoyo del programa Cyber Stewards del Citizen Lab de la Universidad de Toronto en el año 2013.

Este trabajo fue recibido el 24 de marzo de 2014 y aprobado el 16 de junio de 2014.