DELITO DEL ARTÍCULO 2º DE LA LEY Nº 19.223

ESPIONAJE INFORMÁTICO. BIENES JURÍDICOS PROTEGIDOS. APODERAMIENTO, USO Y CONOCIMIENTO INDEBIDO DE LA INFORMACIÓN. FACILITACIÓN EXPRESA DE LA CLAVE DE ACCESO AL CORREO ELECTRÓNICO IMPIDE CALIFICAR EL ACCESO COMO INDEBIDO.

Hechos

El juzgado del crimen absuelve al encausado por el delito de espionaje informático, veredicto que la Corte de Apelaciones confirma. El querellante recurre de casación en el fondo, pero la Corte Suprema desecha su arbitrio procesal.

Antecedentes del fallo:

Tipo: *Recurso de casación en el fondo (rechazado).*
Rol: *Nº 9.238-2012.*
Partes: *"C/Raúl Pérez Rodríguez".*
Ministros: *Sr. Milton Juica Arancibia, Sr. Hugo Dolmestch Urra, Sr. Haroldo Brito Cruz, Sr. Lamberto Cisternas Rocha y Abogado Integrante Sr. Jorge Baraona González.*

Doctrina

El delito de espionaje económico, previsto en el artículo 2º de la Ley Nº 19.223, sanciona el apoderamiento, uso y conocimiento indebido de la información, interfiriendo, interceptando o accediendo al sistema de tratamiento de datos. Protege los bienes jurídicos de privacidad, intimidad y confidencialidad de los datos. En la especie, sin embargo, el encausado por el ilícito aludido no puede ser condenado, sino debe ser absuelto, por cuanto ingresó a la cuenta de correo electrónico del gerente de la empresa querellante luego que éste le diera la clave, situación que impide configurar el elemento "indebidamente", parte del tipo penal en comento. Si bien la autorización no comprendía el reenvío de la información allí contenida, siendo el gerente quien autorizó al acusado a ingresar a su correo electrónico, fue aquél quien puso en peligro los bienes jurídicos que protege el delito en comento (Considerando 3º de la sentencia de la Corte Suprema).

Normativa relevante citada: *artículo 2º de la Ley Nº 19.223.*

Elementos típicos del artículo 2° de la Ley Nº 19.223: Comentario a la SCS de 03.07.2013 Rol Nº 9238-12

Jaime Winter Etcheberry*

Los delitos informáticos, en la legislación chilena, todavía se encuentran en proceso de definir sus contornos concretos, a pesar de los ya 20 años de vigencia de la 19.923 que los tipifica. En ese sentido, la presente sentencia otorga una oportunidad única de discutir sobre los límites y contenido concreto de estos tipos penales.

En particular, el fallo se refiere al artículo 2° de la Ley Nº 19.223, que sanciona 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…*".

La transcripción es necesaria, porque permite observar los elementos que cabe considerar para determinar si existe una infracción a esta norma. Al respecto, sobresalen dos elementos fundamentales: por un lado, interceptar, interferir o acceder a un sistema de tratamiento de datos. Por otro lado, exige un elemento subjetivo particular, consistente en el ánimo de apoderarse, usar o conocer indebidamente la información contenida en dicho sistema. Dichos elementos los observaremos a través de del caso sujeto al conocimiento de la Excma. Corte Suprema, así como la decisión de esta misma.

A grandes rasgos, en el caso en cuestión el imputado accede (y se hará referencia principalmente a la hipótesis típica de "acceder", sin perjuicio de que lo razonado, en general, pueda aplicarse a las hipótesis de interceptar e interferir) al correo del gerente de la empresa en que había dejado de trabajar siete meses antes, reenviándose cierta información. La clave para acceder al correo no fue obtenida de manera fraudulenta, sino que había sido entregada meses antes por la propia víctima al imputado, en el contexto de la relación laboral que los unía.

Si bien los razonamientos de la Excma. Corte, en el sentido de considerar atípica la conducta, se refieren principalmente a la valoración de la prueba, de algún modo se hace eco de lo resuelto en primera instancia (confirmado por la Corte de Apelaciones), en cuanto a que el acceso fue autorizado y que no hay antecedentes que permitan entender que existe una revocación de dicha autorización. Por otra parte, indican también en relación con la sentencia de

* Académico de la Universidad de Chile. Becario DAAD y estudiante de doctorado de la Justus-Liebig-Universität Gießen.

primera instancia, con el fin de la relación laboral, de existir una revocación, cabría esperar que el usuario de la cuenta hubiera tomado alguna medida de seguridad como cambiar la clave. En ese sentido, en términos del tribunal de primera instancia referido por el querellante, el propio gerente puso en peligro los bienes jurídicos. Los argumentos del sentenciador, en esencia correctos, requieren algunas precisiones que se harán al final.

El argumento de la querellante, por el contrario, se refiere a que la autorización que se otorgó al empleado en su momento fue para acceder al correo, no para reenviar la información. Esto, si bien no explicitado en la sentencia, implica una interpretación particular del artículo. En primer lugar, como puede observarse de lo transcrito de la norma penal no pareciera, en principio, ser relevante si el acceso al sistema de tratamiento de datos es en sí mismo indebido. En efecto, lo que se sancionaría es el acceso, sin que se diga que dicho acceso debió haber sido indebido.

Así, lo que caracterizaría a este ilícito no es que el *acceso* al sistema sea ilícito, sino que dicho acceso, que incluso puede ser autorizado, tenga una *finalidad* ilícita. Esa finalidad ilícita está expresada en el requisito subjetivo especial, consistente en el ánimo de apoderarse, usar o conocer *indebidamente* la información. Esto implicaría que lo directamente protegido no es la integridad del sistema de tratamiento de datos, sino que la información contenida en él.

Las consecuencias de aceptar esta interpretación no serían pocas. De partida, lo más relevante es que el ámbito de potenciales individuos capaces de cometer el ilícito se amplía. Una interpretación del ilícito basada en la ilicitud del acceso sólo permite hacer responsables a aquellos que son *extraneus*, es decir, personas ajenas al sistema de tratamiento de datos. Por el contrario, según esta interpretación, el artículo 2° de la Ley Nº 19.223 incluye también al *intraneus*, es decir, aquel que lícitamente puede acceder al sistema.

Por regla general, el *intraneus* tendrá la autorización para conocer el contenido del sistema de tratamiento de datos, de modo que, al menos basado en la hipótesis de conocer, será extraño que pueda considerarse que la persona conoce indebidamente. Sin embargo, en ciertos casos puede configurarse la hipótesis. Se puede pensar, por ejemplo, en el encargado de computación que se le concede acceso a la red de una empresa a efectos de administración, mantención, corrección de errores, etc., y que utiliza dicho acceso para revisar, por ejemplo, documentos sensibles que quienes utilizan el sistema guardan en dicha red. Aquí no es relevante el contenido de los datos, sino que el hecho de que haya una expectativa de que no se acceda a ellos. Por

poner un ejemplo, una carpeta signada como "documentos personales" o "acceso restringido" debiera entenderse como que implica que el ingreso está vedado. Igualmente, reenviarse información de la empresa que no es de libre acceso al público podría entenderse como algo indebido, incluso para quien trabaja en ella.

Sin embargo, esta línea interpretativa no se ajusta a las características de la disposición. Al respecto, resulta interesante revisar la *Historia de la Ley Nº 19.223*, la que aporta interesantes elementos históricos, sistemáticos y teleológicos para entender la prohibición en análisis.

En primer lugar, en la propia moción parlamentaria se expresa que el problema relacionado con los delitos informáticos, en este contexto, no son los bienes jurídicos como la intimidad o el patrimonio que pueden ser atacados mediante medios tecnológicos, sino que "[…] *la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan*".[1-2] En ese sentido, lo esencial es proteger la integridad del sistema de tratamiento de datos. Esto se ve refrendado en cuanto a que durante la Comisión de Constitución, Legislación y Justicia de la Cámara rechazó una indicación del Ejecutivo que veía a los "delitos" informáticos simplemente como medios para cometer otros delitos. En ese sentido, las indicaciones creaban, por ejemplo, el delito de fraude informático[3]. Al rechazar dichas indicaciones la Comisión lo fundamentó en que: "*La Comisión estimó oportuno mantener el texto del proyecto* [es decir, rechazar la indicaciones]*; con la idea matriz de que el sistema automatizado de tratamiento de información, sus partes o componentes, constituyen un bien jurídico que debe ser cautelado por la legislación penal* […]"[4].

Esto se reflejaba con claridad en la formulación original del artículo 2° en análisis, que sostenía: "*El que sin derecho intercepte, interfiera, o acceda a un sistema automatizado de tratamiento de información será castigado con*

[1] *Historia de la Ley Nº 19.223*, p. 4.

[2] Con más claridad todavía Viera-Gallo: "el bien jurídico protegido con el proyecto es un sistema de almacenamiento de información, según la técnica de la informática y no un método para cometer otros delitos". *Historia de la Ley Nº 19.233*, p. 38.

[3] *Historia de la Ley Nº 19.233*, p. 32.

[4] *Historia de la Ley Nº 19.233*, p. 38.

presidio menor en su grado medio".[5] Como se observa, con claridad, lo que se sanciona es el *acceso* sin derecho, no lo que se hace una vez que se accede.
La modificación que en definitiva lleva al texto actual no pretendió en ningún caso modificar ese sentido. En primer lugar, en el mismo sentido que en los otros artículos se utiliza el término "maliciosamente" (al parecer por la discusión parlamentaria, como una forma de evitar la sanción de las hipótesis de negligencia), se introdujo el *propósito* de apropiarse de información ajena indebidamente.
Posteriormente, se acusó que era una redundancia mantener los vocablos de "sin derecho" e "indebidamente"[6], por lo que la Comisión de Constitución, Legislación y Justicia del Senado optó por suprimir "sin derecho", entendiendo que la idea ya estaba contenida en el "indebidamente"[7].
Esto es de la mayor importancia, toda vez que permite entender correctamente el alcance de la inclusión del concepto de "indebidamente". Así, indebidamente no está haciendo referencia la ausencia de un derecho de la persona a conocer, usar o apoderarse de los datos, sino que se refiere al modo de apropiarse dichos datos y éste consiste en realizarlo mediante el acceso, interceptación o interferencia de un sistema de tratamiento de datos. Entonces, apoderarse, usar y conocer indebidamente debe entenderse como apoderarse, usar y conocer, habiendo accedido de manera no permitida al sistema de tratamiento de datos.
Todavía queda, eso sí, determinar qué accesos son *indebidos* en el contexto de la Ley Nº 19.223. Esto debiera ser central en el caso concreto. En efecto, más allá de la discusión probatoria, difícilmente puede decirse que el acceso al sistema que a una persona se le concedió en el contexto de una relación laboral siga vigente una vez que esa relación se acaba e incluso siete meses después. Es decir, el imputado no tenía derecho a ingresar al correo de su ex empleador.
El asunto, sin embargo, es otro. El Tribunal da en con el punto cuando señala que ha sido el propio gerente, al entregar la clave, quien ha puesto en peligro el bien jurídico. Más propiamente, puede decirse que ha sido el gerente quien ha quitado la relevancia penal al asunto. Esto no es un asunto fáctico, donde se sanciona la negligencia del gerente privándolo de protec-

[5] *Historia de la Ley Nº 19.233*, p. 6.

[6] Señalado por el diputado Elgueta en la discusión en Sala en la Cámara. *Historia de la Ley Nº 19.223*, p. 51.

[7] *Historia de la Ley Nº 19.223*, p. 64.

ción penal, sino que es un problema jurídico, donde al entregarse la clave la situación pierde significado penalmente relevante. Esto, porque, como se hace evidente en virtud de la opción del legislador chileno de crear delitos contra sistemas de tratamiento de datos como un objeto de protección en sí mismo, lo relevante a este respecto será que el autor del hecho haya vulnerado los sistemas de seguridad propios del sistema de tratamiento de datos. Con la entrega de la clave, el gerente ha renunciado a esa protección, por lo tanto, ha dejado abierto el acceso al sistema para dicho sujeto. Así, no queda más que entender que la conducta resulta impune.