II. Derecho Penal (parte especial)

1. Corte de Apelaciones - Derecho Penal (Parte especial)

Espionaje informático y difusión maliciosa de información contenida en un sistema de información. Basta para configurar el delito que el agente se limite a "descubrir o manifestar" una información ignorada o se limite a "extender, esparcir o propagar físicamente" ese contenido. Delito se configura al difundir información contenida en la Intranet de la PDI

Hechos

Defensas de los dos sentenciados interponen sendos recursos de nulidad en contra de la sentencia definitiva, que los condenó como autor del delito de espionaje informático y en calidad de autor del delito consumado de difusión maliciosa de información contenida en un sistema de información, respectivamente. Analizado lo expuesto, la Corte de Apelaciones rechaza los recursos de nulidad intentados.

Antecedentes del fallo:
Tipo: *Recurso de nulidad penal (rechazado).*
Tribunal: *Corte de Apelaciones de Santiago.*
Rol: *6010-2019, de 6 de enero de 2020.*
Ministros: Sra. Rosa Kittsteiner Gentile, Fiscal Judicial Sra. Clara Carrasco Andonie y el Abogado Integrante Sr. Gonzalo Ruz Lártiga.

Doctrina

Corresponde a esta Corte evaluar si el tribunal del grado ha hecho una correcta aplicación de la regla del artículo 4º de la Ley Nº 19.223, cuyo tenor expresa lo siguiente: "El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado". Advierte esta Corte, como lo hace el considerando 10º del fallo en análisis, por un lado que, en la descripción típica, la norma utiliza 2 verbos rectores "revelar o difundir", separados de una conjunción disyuntiva "o", lo que supone que basta para configurarla que el agente se limite a "descubrir o manifestar" una información ignorada o secreta (primera acepción del verbo revelar que contiene el diccionario de la Real Academia española de la lengua) o bien se limite a "extender, esparcir o propagar físicamente" ese

contenido (primera acepción del mismo diccionario para el verbo difundir). En el primer caso, lo que se revela no supone única o necesariamente que se trate de información secreta o confidencial, pues también se cumple la acción del verbo rector si esta información es simplemente ignorada por los demás y lo es, si es que, como se acreditó, estaba contenida en la Intranet de la Policía de Investigaciones, que es un sistema informático interno, no de acceso público, que mantiene esa institución exclusivamente para sus componentes. Por otra parte, también comparte esta Corte que el empleo del adverbio "maliciosamente" que contiene la norma que se denuncia como mal aplicada, al contrario de lo dispuesto en el artículo 2º de la misma ley, no exige un ánimo especial, ni que tales conductas deban estar orientadas a un fin específico, como tampoco menciona que deba obtenerse algún tipo de beneficio o gratificación ni la naturaleza de la información, el precepto solo se refiere a la exigencia de dolo directo, es decir, a la simple intención de cometer un hecho contrario a Derecho obteniendo el resultado perseguido, lo que no ha sido discutido en autos, pues ese era el resultado que buscaba –el condenado– al desplegar voluntaria y conscientemente su conducta. Comparte, entonces, esta magistratura, la calificación jurídica que realizan los jueces del grado y no advierte, en consecuencia, que, en su aplicación a los hechos probados en la sentencia, se haya errado en el juicio jurídico (considerandos 14º y 15º de la sentencia de la Corte de Apelaciones).

Cita online: CL/JUR/1214/2020

Normativa relevante citada: *Artículos 373 del Código Procesal Penal; 4º de la Ley Nº 19.223.*

El objeto material del delito del artículo 4º de la Ley Nº 19.223: información no accesible normativamente por terceros

Marcos Contreras Enos

El 18 de octubre de 2019 el Cuarto Tribunal de Juicio Oral en lo Penal de Santiago, en causa RIT 387-2019, RUC 1800024712-6, condenó a dos acusados a sendas penas de 541 y 61 días como autores del delito de difusión maliciosa de información previsto y sancionado en el artículo 4º de la Ley Nº 19.223. Los hechos que se tuvieron por probados consistieron en que uno de los acusados, subcomisario de la Policía de Investigaciones de Chile, procedió al envío desde una cuenta de correo electrónico personal de un mail con 12 archivos adjuntos tipo Excel a la dirección de correo electrónico de otro acusado, exfuncionario policial, quien posteriormente procedió a difundir por la misma vía los archi-

vos adjuntos entre distintas personas con el fin de que fueran subidos a la web. Posteriormente un tercer sujeto procedió a subir los referidos archivos al portal web "Pastebin.com" y también a un perfil de la red social Facebook para, de esta forma, dejar disponible la información a todos sus miembros y a quienes visitaran ese sitio. Los antecedentes contenidos en tales archivos correspondían a información de carácter personal relativa al nombre, grado, fecha de nacimiento y unidad policial de funcionarios de la Policía de Investigaciones de Chile (en adelante e indistintamente, "PDI"), que estaban en el escalafón de Detectives. Posteriormente, el mismo sujeto nuevamente publicó en el sitio web "Pastebin.com", mediante un enlace, un listado con información de carácter personal de funcionarios con grado de Comisarios.

Frente a dicha resolución, las defensas interpusieron recurso de nulidad, el que fue rechazado por la Novena Sala de la Iltma. Corte de Apelaciones de Santiago. Dentro de las diversas causales invocadas, nos interesa concentrarnos en la causal de la letra b) del artículo 373 del Código Procesal Penal respecto del artículo 4º de la Ley Nº 19.223, marco en el cual –más allá de otras consideraciones– se argumentó que la información revelada o difundida no era secreta o confidencial.

La controversia jurídica a analizar, por lo tanto, radica en el objeto material de la conducta, esto es, en qué tipo de información es la que ha de ser objeto de la acción, qué información puede ser difundida o revelada para efectos de la realización del delito del art. 4º de la Ley Nº 19.223. Según los recurrentes, la información que funge como objeto idóneo de la conducta debe ser confidencial o secreta y la información del caso no constaría como tal. La Iltma. Corte de Apelaciones de Santiago niega este aserto sosteniendo que en el caso de la conducta consistente en "revelar" basta para configurar el delito con que el agente se limite a "descubrir o manifestar" una información ignorada o se limite a "extender, esparcir o propagar físicamente" ese contenido. El argumento es el siguiente: "la norma utiliza 2 verbos rectores 'revelar o difundir', separados de una conjunción disyuntiva 'o', lo que supone que basta para configurarla que el agente se limite a 'descubrir o manifestar' una información ignorada o secreta (primera acepción del verbo revelar que contiene el diccionario de la Real Academia Española) o bien se limite a 'extender, esparcir o propagar físicamente' ese contenido (primera acepción del mismo diccionario para el verbo difundir). En el primer caso, lo que se revela no supone única o necesariamente que se trate de información secreta o confidencial, pues también se cumple la acción del verbo rector si esta información es simplemente ignorada por los demás y lo es, si es que, como se acreditó, estaba contenida en la Intranet de la Policía de Investigaciones, que es un sistema informático interno, no de acceso público, que mantiene esa institución exclusivamente para sus componentes".

El art. 4º de la Ley Nº 19.223 no establece como requisito explícito que la información revelada o difundida sea secreta o confidencial (como sí lo hace, por ejemplo, el artículo 246 del Código Penal). La doctrina, en tanto, no es conteste al ponderar si la historia de la ley da cuenta de la exigencia o prescindencia de dicho carácter de la información pertinente[1]. Parte de la doctrina nacional ha emprendido una interpretación teleológico-restrictiva del tipo penal para sostener que la información del artículo 4º debe ser secreta o reservada. Se trata de intentos que, aunque bien inspirados, no se encuentran suficientemente justificados. De este modo, Moscoso, aludiendo al principio de *ultima ratio* y al bien jurídico protegido, sostiene que "[el interés digno de protección penal en los delitos informáticos debería ser la confidencialidad del soporte lógico de un sistema automatizado de la información […] Así, una conducta que no afecte datos confidenciales debe ser eximida de responsabilidad penal por faltar la antijuridicidad material, poniendo en práctica una interpretación restrictiva del tipo[2]. Por su parte, Piedrabuena señala que "[n]o obstante que en la redacción del tipo penal no se señala que los datos sean secretos, una interpretación finalista debe hacernos concluir que sólo deben protegerse o quedar bajo el amparo del tipo penal, aquellos datos que sean de interés por ejemplo económico, estratégico, íntimos, etc., para el sujeto pasivo. Al ocuparse la expresión 'revelar' se confirma dicha apreciación"[3].

De otro lado, la falta de consagración explícita en el artículo 4º del carácter secreto o reservado de la información típicamente relevante ha dado pie para que parte de la doctrina concluya que cualquier tipo de información alojada en

[1] Así, de un lado, Couso señala que "[y]a durante la tramitación del proyecto de ley, iniciado por una moción parlamentaria, quedó en claro el propósito de brindar protección, entre otros aspectos, a la privacidad de los datos contenidos en los sistemas automatizados de información". Couso Salas, Jaime, "Relevancia penal de la intromisión del empleador en los correos electrónicos de sus trabajadores", en *Revista de Derecho. Universidad Católica del Norte*. Año 25, Nº 2 (2018), pp. 60 y 61. De otro lado, Jijena, luego de dar cuenta de los vericuetos de la discusión parlamentaria en torno al carácter de la información, señala que "[l]a conclusión es clara: no se buscó tutelar la intimidad de las personas, nunca se pensó en resguardar garantías relacionadas con su libertad, seguridad y dignidad". Jijena Leiva, Renato, "Debate parlamentario en el ámbito del derecho informático. Análisis de la Ley Nº 19.223, de junio de 1993, que tipifica delitos en materia de sistemas de información", en *Revista de Derecho de la Universidad Católica de Valparaíso*, XV (1993-1994), pp. 358 y ss.

[2] Moscoso Escobar, Romina, "La Ley Nº 19.223 en general y el delito de *hacking* en particular", en *Revista Chilena de Derecho y Tecnología,* vol. 3. Nº 1 (2014), pp. 16-17.

[3] Piedrabuena Richard, Guillermo, "Informe relativo a la diligencia e investigación de los delitos informáticos contemplados en la Ley Nº 19.223 y al fraude informático contenido en el Oficio Nº 422 de 27 de septiembre de 2001". *Boletín de Jurisprudencia. Ministerio Público.* Nº 6 (2001), pp. 86-96.

un sistema de tratamiento de datos puede ser objeto idóneo de la acción[4]. La sentencia comentada, si bien es cierto no llega a sostener eso, asevera que basta con que la información sea ignorada por terceros para ser objeto material de las conductas respectivas. Esa interpretación no es correcta. Ella asume que el mero hecho de que una información se encuentre contenida en un sistema de tratamiento de datos (o aquello, sumado a su ignorancia por parte de tercero), la convierte en información que no puede ser revelada o divulgada so pena de incurrir en una conducta penalmente relevante. Eso implica, de un lado, ponderar de una forma defectuosa los intereses en el marco de la colisión que se produce entre el derecho a la privacidad en su faz de protección de la intimidad de control y la libertad de expresión y, de otro, alterar las coordenadas básicas de la protección de la intimidad en el ordenamiento penal chileno.

Para justificar estos asertos es preciso efectuar una breve clarificación conceptual. De la mano de Bascuñán, corresponde distinguir entre dos facetas de la protección de la intimidad: la intimidad de exclusión y la intimidad de control. Conforme a la primera, la intimidad se concibe como un "derecho de aislamiento expresado en una expectativa de exclusión de otros respecto de ciertos ámbitos personales[5]. Los actos que afectan ese derecho se denominan "atentados de intromisión"[6]. Sin embargo, el derecho a la intimidad no se agota en ello, sino que "también se extiende al control sobre acciones de otros que impliquen alguna forma de uso no consentido de información relativa a la vida personal"[7]. En este caso, se trata de la "intimidad de control" y los actos de afectación de ese derecho se denominan "atentados de indiscreción". Distinguir entre ambos tipos de protección de la intimidad es crucial para entender la relación entre intimidad y libertad de expresión y para llevar a cabo una interpretación del

[4] Lara, Juan Carlos; Martínez, Manuel; Viollier, Pablo, "Hacia una regulación de los delitos informáticos basada en la evidencia", en *Revista Chilena de Derecho y Tecnología*, vol. 3, Nº 1 (2014), p. 111. "[E]l artículo 4 tipifica la revelación o difusión de datos de un sistema informático en general, sin importar si éstos son públicos, y sin exigir que estén bajo secreto, reserva o encriptación, o penando incluso si ya son del conocimiento de quien los recibe. Extremando el caso, bastaría sólo el dolo, o al menos la presencia de un ánimo lucrativo, para configurar el ilícito". En el mismo sentido, pero menos elocuente, Álvarez Fortte, Héctor, "Los delitos informáticos", en *Corpus Iuris Regionis. Revista Jurídica Regional y Subregional Andina* 9 (2009), pp. 122-123.

[5] Bascuñán Rodríguez, Antonio, *Delitos contra la intimidad*, Material docente para uso exclusivo de los estudiantes de la Universidad Adolfo Ibáñez, 3ª versión, revisada, octubre 2019, p. 14.

[6] *Id.*

[7] Bascuñán Rodríguez, *Delitos contra la intimidad*, ob. cit, p. 15.

tipo penal del art 4º de la Ley Nº 19.223 que no altere las coordenadas básicas de la protección penal de la intimidad[8].

En efecto, "[l]a prohibición de actos de intromisión, *en cuanto reconocimiento de una expectativa d*e exclusión, "implica la afirmación de una preponderancia frente a la libertad de información". "Las prohibiciones de intromisión son límites normativos *prima facie* a la libertad de información". Distinto es el caso de las prohibiciones de indiscreción, esto es, las prohibiciones de revelar, divulgar o difundir información de otro, la que se posee legítimamente. "Aquí se trata de una expectativa de control del flujo de la información que otros poseen, sin que esa posesión se haya originado por infracción de prohibición alguna". Sólo excepcionalmente el derecho penal reconoce la expectativa de control, cuando ella se asocia a algún deber especial de confidencialidad por parte de quien obtiene la información cuyo secreto interesa al afectado, que paradigmáticamente es de carácter institucional: el deber del funcionario público, del profesional o del abogado"[9]. La protección de la intimidad de control se encuentra en un conflicto necesario con la libertad de expresión y en el contexto de esa colisión no es evidente que sea un interés por regla general preponderante. De aquí que su protección constitucional no pueda expresarse en términos igualmente categóricos que la protección de la intimidad de exclusión como límite normativo a la libertad de información[10].

Conforme a lo señalado, el delito del art. 4º de la Ley Nº 19.223 ha de ser categorizado como un delito contra la intimidad por indiscreción, es decir, un delito de uso no consentido de información lícitamente obtenida. En cuanto delito de indiscreción, requiere la infracción de un deber de confidencialidad, lo que viene exigido por el tipo penal en cuanto ha de entenderse que "la exigencia de obrar 'maliciosamente' implica el conocimiento de la infracción de un deber de confidencialidad[11]. En efecto, en el marco de esta disposición el término debe entenderse referido "al conocimiento de la concurrencia de los hechos que corresponden al fundamento jurídico de la preponderancia de la protección de

[8] Matus y Ramírez comprenden la dimensión de protección de la intimidad que importa el artículo 4º de la Ley Nº 19.223 al tratarlo bajo la rúbrica "Derecho a la privacidad en internet, Aplicación de la Ley Nº 19.223 y de la Ley General de Telecomunicaciones". Matus Acuña, Jean Pierre; Ramírez Guzmán, María Cecilia, *Manual de Derecho Penal chileno. Parte Especial*, 2ª edición, (Valencia, 2018) pp. 241 y ss.

[9] Bascuñán Rodríguez, Antonio, "Grabaciones subrepticias en el derecho penal chileno. Comentario a la sentencia de la Corte Suprema en el caso Chilevisión II", en *Revista de Ciencias Penales*, XLI-3 (2014), pp. 43-74.

[10] Bascuñán Rodríguez, *Delitos contra la intimidad*, ob. cit, p. 16.

[11] Bascuñán Rodríguez, *Delitos contra la intimidad*, ob. cit., p. 88.

la intimidad frente a la protección de la libertad de expresión, a saber, la obtención de la información bajo un deber especial de confidencialidad"[12]. Abona a la conclusión anterior, el tipo calificado del inciso 2º del artículo 4º, que recibe aplicación en caso de que el autor de la revelación o difusión sea el responsable del sistema de información. Ello ha de entenderse como la consagración de un caso especial de deber de confidencialidad[13].

Queda sentado, por lo tanto, que el delito del artículo 4º presupone un deber de confidencialidad, razón por la cual, para afirmar la tipicidad de la conduta no basta con constatar que la información objeto de la conducta de revelación o divulgación se encontraba alojada en un sistema de tratamiento de datos. Pero tampoco basta con constatar –como lo hace la sentencia comentada– que se trata de información ignorada por terceros. En efecto, para que se pueda afirmar vulneración a una expectativa de control de intimidad (y un correlativo atentado de indiscreción) es preciso constatar la existencia de una expectativa (normativa) de privacidad en relación con la información respectiva. Es por eso que la cuestión no puede resolverse en un plano naturalístico-cognitivo, esto es, respondiendo a la pregunta de si la información *es* ignorada por terceros (como lo hace la sentencia comentada), sino que respondiendo a la cuestión normativa consistente en si esa información *debe* mantenerse siendo ignorada por terceros, es decir, fuera de su conocimiento. Formulada de otra forma, la cuestión pertinente no es la de la accesibilidad fáctica, sino la de la accesibilidad normativa por parte de terceros (¿se tiene derecho por parte de ellos a acceder a la información?). Lo anterior se responde con base en la consideración de la naturaleza de la información y no del lugar donde ella se encuentra: el lugar donde se aloja la información (en este caso una intranet institucional de la PDI) no hace operar una alquimia de la naturaleza de la información, de modo tal que la información que en sí misma es pública (esto es, respecto de la cual no hay expectativas normativas de intimidad de control) se transforme en reservada, secreta o confidencial por su adscripción a un sistema de tratamiento de datos. Es preciso, además, poder afirmar que existía un deber de confidencialidad y que ese deber alcanzaba precisamente a la información objeto del caso. Este segundo aspecto se traduce en la pregunta acerca de si la información se encuentra accesible normativamente a terceros, toda vez que respecto de esa información no hay una expectativa normativa de control ni,

[12] Bascuñán Rodríguez, *Delitos contra la intimidad*, ob. cit., p. 89.

[13] *Id.*

por lo tanto, un deber de confidencialidad[14]. Esa es la pregunta que la sentencia comentada debió haber respondido y que ni siquiera se formuló.

En pos de responder esa pregunta debiera al menos considerarse que la regla general en materia de indiscreción es el derecho a informar, salvo que se trate de los casos excepcionales establecidos en la ley en los que se haga preponderar la protección de la vida privada por sobre ese derecho. En el ámbito público, además, hay que considerar el *topos* de la publicidad establecido en el artículo 8º de la Constitución Política de la República. También hay que atender a lo dispuesto en la Ley Nº 20.285 "Sobre acceso a la información pública", en sus artículos 1º[15], que determina el objeto de la ley –la regulación del principio de transparencia de la función pública– y 2º[16], que hace aplicable las disposiciones de dicho cuerpo normativo a la PDI. Por lo demás, debe observarse lo dispuesto en el artículo 10, que establece de forma amplia el derecho a solicitar información de los órganos del Estado y el alcance material del mismo[17] y el artículo 11 que establece para efecto de ese derecho, principios tales como el de relevancia (presumiéndose ésta respecto de toda información que posean los órganos del Estado)[18], el de la libertad

[14] A este respecto es necesario formular un matiz. En algunos casos podría afirmarse que hay vulneración a la intimidad a pesar de que la información bruta sea accesible normativamente a terceros, pero en los que el tratamiento que ha recibido esa información bruta sea aquello que exponga la intimidad.

[15] "La presente ley regula el principio de transparencia de la función pública, el derecho de acceso a la información de los órganos de la Administración del Estado, los procedimientos para el ejercicio del derecho y para su amparo, y las excepciones a la publicidad de la información".

[16] "Artículo 2º.- Las disposiciones de esta ley serán aplicables a los ministerios, las intendencias, las gobernaciones, los gobiernos regionales, las municipalidades, las Fuerzas Armadas, de Orden y Seguridad Pública, y los órganos y servicios públicos creados para el cumplimiento de la función administrativa".

[17] "Artículo 10.- Toda persona tiene derecho a solicitar y recibir información de cualquier órgano de la Administración del Estado, en la forma y condiciones que establece esta ley.

El acceso a la información comprende el derecho de acceder a las informaciones contenidas en actos, resoluciones, actas, expedientes, contratos y acuerdos, así como a toda información elaborada con presupuesto público, cualquiera sea el formato o soporte en que se contenga, salvo las excepciones legales".

[18] Artículo 11.- a) Principio de la relevancia, conforme al cual se presume relevante toda información que posean los órganos de la Administración del Estado, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento.

de información[19], el de apertura o transparencia[20] y el de máxima divulgación[21]. Todos estos principios establecen, de la forma más amplia posible, el derecho de terceros a acceder a información pública, salvo en los casos exceptuados en la ley, los que se encuentran establecidos en el artículo 21 de la Ley Nº 20.285[22]. Finalmente, también podría venir en consideración lo dispuesto en el artículo 7º de la Ley Nº 19.628 "Sobre protección de la vida privada", que establece el deber de guardar secreto para las personas que trabajan en el tratamiento de datos personales solo en cuanto provengan o hayan sido recolectados de fuentes no accesibles al público.

En razón de lo anterior, si la información revelada y divulgada por los acusados (nombre, grado, fecha de nacimiento y unidad policial de funcionarios

[19] b) Principio de la libertad de información, de acuerdo al que toda persona goza del derecho a acceder a la información que obre en poder de los órganos de la Administración del Estado, con las solas excepciones o limitaciones establecidas por leyes de quórum calificado.

[20] c) Principio de apertura o transparencia, conforme al cual toda la información en poder de los órganos de la Administración del Estado se presume pública, a menos que esté sujeta a las excepciones señaladas.

[21] d) Principio de máxima divulgación, de acuerdo al que los órganos de la Administración del Estado deben proporcionar información en los términos más amplios posibles, excluyendo sólo aquello que esté sujeto a las excepciones constitucionales o legales.

[22] Artículo 21.- Las únicas causales de secreto o reserva en cuya virtud se podrá denegar total o parcialmente el acceso a la información, son las siguientes:

1. Cuando su publicidad, comunicación o conocimiento afecte el debido cumplimiento de las funciones del órgano requerido, particularmente:

a) Si es en desmedro de la prevención, investigación y persecución de un crimen o simple delito o se trate de antecedentes necesarios a defensas jurídicas y judiciales.

b) Tratándose de antecedentes o deliberaciones previas a la adopción de una resolución, medida o política, sin perjuicio que los fundamentos de aquéllas sean públicos una vez que sean adoptadas.

c) Tratándose de requerimientos de carácter genérico, referidos a un elevado número de actos administrativos o sus antecedentes o cuya atención requiera distraer indebidamente a los funcionarios del cumplimiento regular de sus labores habituales.

2. Cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico.

3. Cuando su publicidad, comunicación o conocimiento afecte la seguridad de la Nación, particularmente si se refiere a la defensa nacional o la mantención del orden público o la seguridad pública.

4. Cuando su publicidad, comunicación o conocimiento afecte el interés nacional, en especial si se refieren a la salud pública o las relaciones internacionales y los intereses económicos o comerciales del país.

5. Cuando se trate de documentos, datos o informaciones que una ley de quórum calificado haya declarado reservados o secretos, de acuerdo a las causales señaladas en el artículo 8º de la Constitución Política.

de la PDI) es de aquella información que debe ser entregada por el respectivo organismo en el marco de sus obligaciones de transparencia activa o pasiva, por no encontrarse sujeta a algunas de las prohibiciones legales, puede afirmarse accesibilidad normativa de terceros en relación con ella y, correlativamente, negarse una expectativa normativa de intimidad de control por parte de las personas a quienes se referían los datos. El razonamiento decisorio del fallo debiera haber versado sobre ello.