Revista de Derecho
Universidad Católica del Norte
Sección: Estudios
Año 25 - Nº 2, 2018
pp. 29-76

Relevancia penal de la intromisión del empleador en los correos electrónicos de sus trabajadores*

Jaime Couso Salas**

Resumen: El artículo examina qué protección ofrece la legislación penal chilena a los correos electrónicos de los trabajadores, con especial referencia a los enviados o recibidos por medio de cuentas proporcionadas por el empleador al trabajador para el desempeño de sus funciones. Partiendo del reconocimiento que el Tribunal Constitucional ha hecho de que la inviolabilidad de las comunicaciones también se extiende a los correos y documentos electrónicos, a continuación se examina si la intromisión del empleador es penalmente relevante, en relación con los diversos tipos penales que, en una primera aproximación, parecen ser aplicables –teniendo en cuenta además, para ilustrar los problemas interpretativos que se plantean, el derecho comparado de Alemania y otras legislaciones afines–. También se examina si el interés del empleador en prevenir o sancionar hechos que afectan los intereses de la empresa podría justificar penalmente la conducta.

Palabras clave: protección penal; correo electrónico; inviolabilidad de las comunicaciones; servicios públicos de telecomunicaciones; sistemas de tratamiento de información.

* Fecha de recepción: 13 de septiembre de 2016.
Fecha de aceptación: 14 de julio de 2017.

** Doctor en Derecho por la Universidad de Sevilla (España), Profesor Titular de Derecho Penal, Universidad Diego Portales. República 112, Santiago (Chile). Correo electrónico: jaime.couso@mail.udp.cl

Agradezco los valiosos comentarios y sugerencias hechos a una versión anterior de este trabajo por mis colegas Mauricio Duce, Héctor Hernández, Fernando Londoño, Domingo Lovera, Cristián Riego, José Luis Ugarte y Tomás Vial, en un seminario de discusión de *papers* celebrado en la Facultad de Derecho de la Universidad Diego Portales. También agradezco las muy atendibles observaciones hechas por los árbitros anónimos de la Revista de Derecho Universidad Católica del Norte (RDUCN).

Criminal liability of the employer for intruding into his employee's emails

Abstract: The paper examines the protection granted by Chilean criminal law to the employee's emails, with special reference to those sent or received through email accounts provided by the employer for official use by the employee. Starting from the fact that Chilean Constitutional Court in has extended the inviolability of communications to emails and electronic documents, the paper further examines if the employer's intrusion is punishable under criminal law, having in mind the variety of crimes that *prima facie* seem applicable. Besides, attention is given to comparative law from Germany and other legal systems akin to it, in order to shed light upon interpretive issues. Furthermore, it is examined if the employer's intention to protect the company's interests could justify the conduct under the criminal law.

Key words: criminal protection; email; privacy of communications; public telecommunication transport services; information processing systems.

Sumario: Introducción. 1) Panorámica de la protección penal de la intimidad y de la inviolabilidad de las comunicaciones privadas en el ordenamiento jurídico chileno. 2) Protección constitucional de inviolabilidad de los correos electrónicos. El caso de las cuentas habilitadas por el empleador. 3) Protección penal de los correos electrónicos del trabajador frente a intromisiones del empleador. (3.1.) Intervención y difusión de comunicaciones privadas, del artículo 161-A del CP (3.2.) Apertura o registro de la correspondencia o de los papeles de otro. (3.2.1.) Primera modalidad: apertura de cartas. (3.2.2.) Segunda modalidad: registro de papeles (3.2.3.) Calificación por la divulgación de los secretos descubiertos. (3.3.) Captación y difusión de comunicaciones sostenidas a través de servicios públicos de telecomunicaciones, y acceso no autorizado y revelación de datos de un sistema de tratamiento de información. (3.3.1.) Los correos electrónicos, su forma de operación y las alternativas para la intromisión en ellos. (3.3.2.) Captación y difusión de comunicaciones sostenidas a través de servicios públicos de telecomunicaciones, del artículo 36 B, letras c) y d), de la Ley de Telecomunicaciones. (3.3.3.) Acceso no autorizado y revelación de datos contenidos en sistemas de tratamiento de información, de los artículos 2° y 4° de la Ley de Delitos Informáticos. (3.4.) Falta de autorización o de voluntad por parte del titular de los datos o comunicaciones. 4) Posible concurrencia de una causal de justificación. Conclusiones. Bibliografía y Jurisprudencia citada.

Introducción

El desarrollo de las telecomunicaciones y la informática ha hecho del correo electrónico –entre otras formas de comunicación electrónica– un instrumento de importancia fundamental, tanto en la vida privada de las personas como en su actividad laboral. Y el hecho de que ellas suelan emplear una única y misma cuenta de correo electrónico para entablar ambas especies de comunicación plantea cuestiones relevantes acerca del estatuto penal de las posibles intromisiones en tales comunicaciones por parte de los empleadores, quienes pueden tener interés patrimonial en conocer su contenido cuando las comunicaciones se producen en un contexto laboral.

En efecto, si bien parece haber acuerdo en que la inviolabilidad de las comunicaciones privadas se extiende a los correos electrónicos, y una doctrina penal incipiente –y casi sin excepción, a través de manuales de Parte Especial– entiende que son aplicables al efecto los tipos penales que protegen las señales de telecomunicaciones y los sistemas de tratamiento de información, el déficit de tratamiento monográfico y jurisprudencial de la cuestión, unido a la falta de mención explícita a los correos electrónicos en la legislación, justifican el ejercicio de volver a plantearse las preguntas más básicas, a saber, si acaso está penalmente protegido el correo electrónico y a través de qué tipos penales, para luego, a partir de las respuestas a esa pregunta, plantearse cuestiones más específicas sobre el alcance y límites que encuentra esa protección en contextos en que las comunicaciones privadas de los trabajadores pueden confundirse, a través de un mismo medio, con comunicaciones relativas a su actividad laboral. En particular, si el correo electrónico efectivamente goza de protección penal, ¿supone un límite a dicha tutela la circunstancia, cada vez más común, de que haya sido la empresa la que puso la cuenta de correo electrónico a disposición del trabajador para el desempeño de sus funciones, y que los respaldos de los correos electrónicos queden almacenados en computadores de propiedad de aquella? ¿Y se encuentra justificada la intromisión por el hecho de que la empresa se proponga prevenir hechos que atentan contra sus intereses, o perseguir la responsabilidad de los trabajadores por tales hechos?

El artículo se propone responder a esas preguntas, teniendo en cuenta los diversos tipos penales que, en una primera aproximación, podrían reclamar aplicación, y considerando, para ilustrar los problemas interpretativos que se plantean, el derecho comparado, en particular, el derecho alemán y algunas otras legislaciones afines. En todo caso, aun cuando

la inviolabilidad de las comunicaciones entabladas a través de correos electrónicos ha sido afirmada –en la jurisprudencia constitucional– sin distinguir debidamente entre contextos estrictamente laborales y contextos relativos a la función pública, en este trabajo la atención estará puesta exclusivamente en los primeros contextos.

El análisis comenzará con una síntesis panorámica sobre la forma en que el derecho penal chileno protege las garantías constitucionales de la intimidad[1] y la inviolabilidad de las comunicaciones (1), un análisis del alcance de tal protección a las comunicaciones y documentos en soporte electrónico, con especial referencia a los correos electrónicos enviados desde y recibidos en casillas o cuentas habilitadas por el empleador para que el trabajador desempeñe sus funciones (2), un examen de la posible tipicidad de la intromisión del empleador en los correos electrónicos del trabajador, en relación con los diversos tipos penales que en principio parecen relevantes (3), un breve examen de las posibles causas de justificación que podría invocarse (4), y unas conclusiones finales (5).

1) Panorámica de la protección penal de la intimidad y de la inviolabilidad de las comunicaciones privadas en el ordenamiento jurídico chileno

De forma relativamente sucinta, a continuación se ofrece una panorámica de las diversas dimensiones de la protección brindada por la legislación penal a las garantías constitucionales de la intimidad de las personas y de la inviolabilidad de las comunicaciones privadas.

El antecedente constitucional de la protección penal brindada por las diversas figuras típicas relevantes en este ámbito se encuentra en el artículo 19, números 4° y 5° de la Constitución Política de la República, que aseguran a todas las personas, respectivamente, "[*e*]*l respeto y protección a la vida privada y a la honra de la persona y su familia*" y "[*l*]*a inviolabilidad del hogar y de toda forma de comunicación privada*"[2].

---

1 En este artículo no se examina la posibilidad de distinguir conceptualmente entre intimidad y privacidad, que excede de los propósitos del mismo. Se utilizan ambos conceptos más o menos indistintamente, siendo clara cuál es la referencia normativa.

2 V. Medina, Gonzalo (2008) "Algunos aspectos de la protección penal de la privacidad". En Fernández Cruz, José Ángel (Coordinador). *Estudios de Ciencias Penales. Hacia una racionalización del Derecho Penal*. Santiago: LegalPublishing, pp. 241-262, 245, 246, derivando de estas normas constitucionales los diversos aspectos de la "privacidad" (término que emplea como género común a lo que aquí se identifica como "intimidad" e "inviolabilidad de las comunicaciones privadas") que luego encuentran protección penal. En las obras generales sobre la Parte Especial del Derecho Penal también suele ofrecerse este encuadre jurídico-

Una primera distinción ilustrativa acerca de la forma como el Derecho penal protege la vida privada y la inviolabilidad de las comunicaciones privadas es la que reconoce, por una parte, prohibiciones de actos de "intromisión", y por la otra, prohibiciones de actos de indiscreción[3]. Los delitos de intromisión protegen un interés o expectativa "de intimidad" o "de exclusión de otro en el ámbito propio de comunicación", que se frustra mediante el "ingreso o acceso al ámbito de comunicación de otro, no consentidos por este", mientras que los delitos de indiscreción protegen un interés o expectativa de "control sobre el flujo de la información que otros poseen", que se frustra mediante "la extensión del ámbito de comunicación de otro, no consentido por este", a través de la revelación, exhibición, divulgación o difusión de información que se posee legítimamente[4] [5].

Aunque la protección frente a ambas formas de atentado en contra de la intimidad y la inviolabilidad de las comunicaciones es fragmentaria, sin abarcar en caso alguno todos sus ámbitos, ese rasgo se vería acentuado en relación con los delitos de indiscreción, a falta de un deber general de discreción frente a la intimidad de otros –solo se puede apreciar un deber especial de discreción, que recae en un círculo restringido de destinatarios–; deber general que sí existiría, en cambio, en relación con la abstención de actos de intromisión[6].

Este artículo examinará precisamente actos de intromisión en la intimidad.

En una primera mirada[7], la legislación penal protege la intimidad y la inviolabilidad de las comunicaciones o documentos privados, en contra de actos de intromisión, en dos tipos de contextos o circunstancias que dan cuenta de una expectativa de exclusión de otros:

constitucional; véase Etcheberry, Alfredo (1998) *Derecho Penal. Parte Especial.* 3ª edición revisada y actualizada. Santiago: Editorial Jurídica de Chile. Tomo III, p. 252.

3 Así, Bascuñán Rodríguez, Antonio (2005) "Delitos contra los intereses personalísimos", *Revista de Derecho de la Universidad Adolfo Ibáñez*, Número 2, pp. 531-556, 548; y, más recientemente, del mismo autor, (2014) "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, Sexta época, Vol. XLI, N° 3, pp. 43-74, 51, 53.

4 Bascuñán Rodríguez (2005) 548, Bascuñán Rodríguez (2014) 53.

5 En cambio, los delitos calificados por la divulgación de la información obtenida a través de un delito de intromisión, serían también delitos de intromisión, cuya ilicitud es "derivativa" de la obtención ilícita de la información; no constituirían entonces, pese a su similitud fenoménica, un delito de "indiscreción"; véase Bascuñán Rodríguez (2014) 53 y nota 21.

6 Bascuñán Rodríguez (2005) 549. Bascuñán Rodríguez (2014) 52-53.

7 Para más detalles, véase *infra* 3., donde se transcriben además las disposiciones legales más relevantes.

1) cuando se trata de comunicaciones o documentos cuyo soporte o continente, físico o electrónico, impide su percepción directa por terceros (por más que sea un impedimento fácil de vencer sin autorización), sin importar si las comunicaciones o documentos están referidos a un aspecto de la "intimidad" de las personas (artículos 146 del CP, 2º y 4° de la Ley de Delitos Informáticos y 36 B, letras c) y d), de la Ley de Telecomunicaciones); y
2) cuando se trata de comunicaciones, documentos o hechos que, sin contar con un soporte o continente, se encuentran o se producen dentro de recintos o lugares que no están abiertos al público (por más que sean recintos a los que es fácil entrar sin autorización) y son, además –en un sentido que requiere aclaración– "privados" (artículo 161-A del CP).

Sin perjuicio de las "lagunas de punibilidad", apreciables en otros ámbitos[8], si se atiende exclusivamente a la protección de la inviolabilidad de las comunicaciones y de documentos privados, aquel conjunto de tipificaciones ofrece instrumentos para una amplia tutela penal, sin restricciones importantes respecto del tipo de soporte o de contexto mediante el cual se expresa la pretensión de tratar unas y otros como "privados", es decir, la pretensión de excluir a otros: por una parte, resguardos físicos o técnicos de los objetos protegidos, que claramente dan cuenta de esa pretensión, al impedir la percepción directa; por otra, el confinamiento de los objetos protegidos a recintos no accesibles por terceros no autorizados, que expresan la misma pretensión. Esos recursos para conferir privacidad a conversaciones y documentos no tienen el sentido de hacer especialmente difícil el acceso ("nada más simple que abrir una carta", ha argüido el Tribunal Constitucional chileno, en este mismo sentido[9]), sino

8 Critican el carácter fragmentario, en este sentido, de la protección penal de la "privacidad" o "intimidad", respectivamente, Medina (2008) 254; y, Bascuñán Rodríguez (2005) 550. Crítico, también, ya Etcheberry (1998) 276. Un ámbito que queda claramente sin protección penal es el de las comunicaciones o documentos apreciables directamente por los sentidos, que se produzcan o se encuentren en recintos que permiten acceso más o menos libre a terceros a quienes no se ha autorizado a conocer la información. Es discutible si acaso consideraciones afines a la "víctimo-dogmática", que exigen una cuota mínima de "autocuidado" por parte de la víctima, antes de dispensarle protección penal, justifican esta "laguna de punibilidad" en ciertos casos. Un hecho relativamente reciente acontecido en la Cámara de Diputados, cuando un periodista fotografió la pantalla del teléfono celular de un diputado, en la que podía apreciarse el texto de un mensaje referido a su vida íntima, que este se disponía a enviar a destinatarios determinados, parece encontrarse en ese ámbito en que las garantías constitucionales de la vida privada y de la inviolabilidad de toda forma de comunicación privada no encontrarían un correlato en la tutela penal. Fuera de ello, sobre las lagunas que presenta el Art. 161-A del CP; véase Bascuñán Rodríguez (2005) 550.

9 Tribunal Constitucional. 29 de enero de 2014. Rol N° 2379-13-INA. Disponible en: https://www.camara.cl/sala/verComunicacion.aspx?comuid=10871 [fecha de visita: 15 de

el de expresar la expectativa de privacidad, cuya extensión cada individuo es soberano para definir a través del recurso a alguno de estos medios (cerrando el sobre, guardando el documento, enviando el correo electrónico o el SMS a un círculo definido de destinatarios, archivando el documento en el computador que usa, o conversando privadamente en el living de su casa).

Ahora bien, dado que el Derecho penal no solo debe verse como un instrumento de tutela de los bienes jurídicos directamente afectados por los delitos, sino también como una garantía, a favor de los destinatarios de las prohibiciones penales y las penas, de que esa tutela solo se efectuará a costa de un individuo si la conducta que ha realizado está tipificada, todavía hay que examinar, de la mano de cada una de las disposiciones indicadas, si acaso la conducta que es objeto de análisis por este artículo cumple con las exigencias típicas, y si acaso, al menos en un primer examen, no se encuentra justificada por el contexto o las razones que podrían motivarla.

Pero, antes de entrar en ese análisis, es necesario despejar una cuestión conceptual: si acaso, y en qué medida, las comunicaciones entabladas a través de correos electrónicos proporcionados al trabajador por la empresa, como un instrumento de trabajo, y los documentos alojados en servidores o computadores que se encuentren en la misma situación, pueden reclamar el estatuto propio de las comunicaciones y documentos privados.

2) Protección constitucional de la inviolabilidad de los correos electrónicos. El caso de las cuentas habilitadas por el empleador

En la actualidad no parece haber dudas acerca de que los correos electrónicos y documentos contenidos en un soporte electrónico son objetos protegidos por las garantías constitucionales de los números 4º y 5º del artículo 19 de la Constitución[10]. También parece estar consolidada la

noviembre de 2015] considerando trigésimo, argumentando que los correos electrónicos son comunicaciones privadas, y que expresan "*una expectativa razonable de que están a cubierto de injerencias y del conocimiento de terceros*", y que "nada obsta a lo anterior el que no sea muy dificultoso interceptarlos o abrirlos", pues, precisamente las cartas, cuyo carácter privado está fuera de duda, pueden ser abiertas sin ninguna dificultad.

10 En el caso de los correos electrónicos, así lo ha reconocido el Tribunal Constitucional, ya claramente en la sentencia del Tribunal Constitucional. 11 de septiembre de 2011. Rol N° 2153-11-INA. Disponible en: http://www.tribunalconstitucional.cl/wp/wp-content/uploads/Rol-N-2153-correos-electr%C3%B3nicos-a-firma.pdf [fecha de visita: 15 de no-

doctrina que sostiene que esa protección es independiente de la propiedad sobre el *hardware* o soporte material en los que se contengan los datos o sobre el servidor a través del cual se transmitan o reciban los correos electrónicos[11], lo que interesa especialmente en el caso de los documentos o comunicaciones de trabajadores contenidos en un *hardware* o realizadas a través de un servidor de propiedad del empleador, sobre todo desde que la autoridad administrativa y el Tribunal Constitucional debieron pronunciarse sobre el asunto.

La Dirección del Trabajo, en efecto, en a lo menos dos ocasiones ha debido resolver si los empleadores, tienen la facultad de acceder a los mensajes de correo electrónico de los trabajadores, enviados y recibidos a través de los servicios y casillas o cuentas habilitados por los propios empleadores como una herramienta de trabajo, pronunciándose en ambos casos categóricamente de forma negativa.

Así, en 2002, enfrentada a la necesidad de resolver el conflicto entre "la garantía constitucional de inviolabilidad de toda forma de comunicación privada" y "la facultad del empleador de organizar, dirigir y administrar su empresa, que emana de la garantía constitucional del derecho de propiedad", asimiló las cuentas de correo electrónico facilitadas por el empleador al trabajador a las líneas telefónicas y los cajones del escritorio que pone a su disposición, que naturalmente son "una extensión de la persona y actividad del dependiente", no sujeto a control, resolviendo que:

> *"[…] de acuerdo a las facultades con que cuenta el empleador para administrar su empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos de la empresa, pero en ningún caso podrá tener acceso a la correspondencia electrónica privada enviada y recibida por los trabajadores"*[12].

viembre de 2015] considerando 42°: "los correos electrónicos se enmarcan perfectamente dentro de la expresión "comunicaciones y documentos privados" que utiliza el artículo 19 N° 5° de la Constitución". También así lo ha entendido la doctrina; véase, por todos, ya Álvarez Valenzuela, Daniel (2005), "Inviolabilidad de las comunicaciones electrónicas", *Revista Chilena de Derecho Informático*, Nº 5, pp. 191-202, 197.

11 Así, Álvarez Valenzuela (2005) 198-199. Ahora bien, que la privacidad del trabajador encuentre protección aun frente a la propiedad del empleador, no supone negar la posibilidad de colisiones entre ambos intereses, que eventualmente han de ser ponderados; así, Ugarte Cataldo, José Luis (2011) "Privacidad, trabajo y derechos fundamentales", *Estudios Constitucionales*, Año 9, Nº 1, pp. 13-36, 23 (si bien refiréndose, en lo pertinente, a hipótesis distintas del la intromisión en los correos electrónicos del trabajador). En materia penal, ello podría ser relevante para resolver si una intromisión –penalmente típica– en los correos electrónicos puede estar en el caso concreto amparada por una causa de justificación; véase *infra*, 4.

12 Dictamen de la Dirección del Trabajo Ord. Nº 260/019 de 24 de enero de 2002.

Y añadió que el reglamento interno de la empresa, o el contrato de trabajo podrán "regular, limitar o restringir el empleo de los correos electrónicos", pero "no […] la garantía constitucional de la inviolabilidad de la correspondencia", de modo que, en una opción radical por parte del empleador, podrá exigirse que todo envío de correos electrónicos del personal se efectúe con copia a alguna gerencia o unidad de la empresa, "envío que de esta forma perderá –en el instante– su condición de *comunicación privada*, regulación que sin embargo no es practicable en el caso de la recepción de correspondencia electrónica, y por tanto, en este aspecto, esta modalidad de comunicación conserva siempre su carácter *privado*"[13]. resolución que, en realidad, también parece reconocer la protección de todo correo electrónico enviado por el trabajador sin copia a la empresa.

Tres años después, al pronunciarse sobre una solicitud de reconsideración del Dictamen anterior, la Dirección del Trabajo reitera su doctrina, aclarando por lo demás que la prohibición de acceso a los correos electrónicos del trabajador se refiere también a los enviados por este:

> *"En consecuencia, de la inviolabilidad citada se seguiría la imposibilidad de que la empresa revise el contenido de los correos electrónicos de sus trabajadores, tanto los enviados como los recibidos, sin perjuicio de la facultad empresarial de regular el acceso y el envío de dichos correos electrónicos, como establecer restricciones sobre el uso de dichos correo [sic] en la empresa"*[14].

La protección constitucional de la inviolabilidad de los correos electrónicos de los trabajadores, con independencia de la propiedad sobre el servidor o servicio a través del cual se transmiten y del carácter oficial –y no particular– de la cuenta o casilla empleada, también ha sido afirmada por el Tribunal Constitucional, incluso con preponderancia sobre intereses que podrían considerarse de mayor peso que la propiedad del empleador sobre aquellos servidores o servicios: la transparencia de los actos de la administración.

Así, en 2014, el Tribunal Constitucional, siguiendo la doctrina anticipada en decisiones anteriores[15], declaró la inaplicabilidad por inconstitucionalidad del artículo 5º, inc. 2º, de la Ley Nº 20.285, sobre Acceso a la Información Pública[16], por afectar la garantía de la inviolabilidad de

13 Dictamen D. del Trabajo Ord. N° 260/019 (las cursivas están en el original).
14 Dictamen de la Dirección del Trabajo Ord. Nº 1147/34, de 21 de marzo de 2005.
15 La primera de ellas, la sentencia del TC. Rol N° 253-11-INA.
16 TC. Rol N° 2379-13-INA.

las comunicaciones privadas, del Art. 19, nº 5º, de la Constitución, sosteniendo que:

> *"[N]ada cambia por el hecho de que el funcionario utilice un computador proporcionado por la repartición, una red que paga el Estado y una casilla que le asigna el organismo respectivo. Desde luego, porque nadie diría que las conversaciones telefónicas, por el hecho de realizarse por un teléfono que proporciona el servicio, cuya interconexión cancela el mismo, pueden escucharse, grabarse y/o difundirse*[17].

Y sobre las facultades de control que al Estado le confiere el hecho de que se trate de una cuenta proporcionada por este, como instrumento para el cumplimiento de funciones públicas, descarta que ello se oponga al uso privado, arguyendo que:

> *"el Estado pone a disposición de los funcionarios una serie de bienes que pueden usarse con distintos propósitos. Una serie de bienes de la modernidad que se ponen a disposición de los funcionarios no pueden ser interpretados con los criterios de antaño, definidos para otros bienes […] hay que considerar que cabe un uso legítimo de mensajes personales ineludibles"*[18].

Y concluye que *"[l]o que se debe prevenir siempre es el mal uso, porque eso afecta la probidad"*[19].

Fuera de ello, a los correos electrónicos se aplica el criterio de la irrelevancia de su contenido para decidir la ilicitud del acto de intromisión, tal como ocurre con las cartas[20]:

> *"El carácter inviolable de la comunicación no tiene que ver tampoco con el contenido de la misma. Se protege el mensaje, sea que tenga que ver con aspectos públicos o privados, sea que se refieran a aspectos trascendentes o intrascendentes, afecten o no la vida privada. Este derecho no se entrega en virtud del contenido de la comunicación; no tiene que ver con el carácter confidencial o privado de lo que se transmite"*[21].

---

17 TC. Rol N° 2379-13-INA, considerando 31º.
18 TC. Rol N° 2379-13-INA, considerando 31º.
19 TC. Rol N° 2379-13-INA, considerando 31º.
20 Véase *infra* 3.2.3, donde es clara la punibilidad de la apertura de cartas aun si no contienen "secretos".
21 TC. Rol N° 2379-13-INA, considerando 29º.

En esta afirmación del Tribunal Constitucional, con todo, hay que distinguir entre el –justificado– reconocimiento de protección constitucional a los mensajes de correo electrónico, por el solo hecho de haber sido dirigidos a –o desde– una cuenta asignada individualmente al trabajador (también el trabajador que se desempeña en el sector público), de la –injustificada– pretensión, que parece deslizarse en esa cita, de que el carácter o relevancia pública de la información que contienen o podrían contener los correos electrónicos de un funcionario público no hace ninguna diferencia a la hora de justificar una intromisión. En relación con el primer aspecto, el Tribunal Constitucional acierta al entender que los correos electrónicos son comunicaciones privadas –protegidas constitucionalmente– simplemente por el hecho de que "el emitente singulariza al o a los destinatarios de su comunicación con el evidente propósito de que solo él o ellos la reciban"[22], y sin importar que los servidores a través de los cuales esas comunicaciones tienen lugar o los computadores con los cuales se accede a ellos hayan sido proporcionados al funcionario (o trabajador) con fines oficiales o laborales. Pero a la hora de examinar si el interés constitucional en proteger la privacidad de los correos electrónicos ha de ceder frente a otros intereses preponderantes no se puede ignorar que, en el caso de los funcionarios públicos, no se trata solo de intereses propietarios del empleador (el empleador público también puede tenerlos), sino también, con frecuencia, de intereses públicos muy relevantes, como el control democrático del ejercicio del poder político y la transparencia de los actos de la Administración. En este trabajo, con todo, como se advirtió en la introducción, no se aborda esta dimensión de la cuestión, concentrándose la atención, en cambio, en la intromisión del empleador en los correos electrónicos del trabajador que no desempeña una función pública; intromisión que, en cualquier caso, no obstante constituir afectación de la privacidad, también podría estar excepcionalmente justificada[23].

3) Protección penal de los correos electrónicos del trabajador frente a intromisiones del empleador

A continuación se examina, respecto de cada una de las disposiciones penales ya individualizadas, si acaso la intromisión del empleador en los correos electrónicos de un trabajador satisface las respectivas exigencias

22 TC. Rol N° 2379-13-INA, considerando 29º.
23 Véase, al respecto, *infra* 4.

típicas. En primer lugar se examinará muy brevemente el tipo del artículo 161-A del CP, para descartar su aplicación a este tipo de hechos (3.1). En seguida se examinará el tipo del artículo 146 del CP, para concluir que, si bien desde el punto de vista de su alcance semántico es capaz de abarcar las intromisiones de terceros en los correos electrónicos, una consideración sistemática –iluminada por un examen del derecho comparado– lleva a la conclusión opuesta (3.2). En efecto, en la medida que se considere aplicables a los correos electrónicos los tipos penales de la Ley de Telecomunicaciones y de la Ley de Delitos Informáticos (como se sostiene en la sección 3.3), entonces el artículo 146 del CP dejaría de serlo; en cambio, quien sostenga que aquellos tipos no son aplicables, no debería encontrar obstáculos para brindar a los correos electrónicos la protección que el artículo 146 del CP brinda a las cartas y papeles.

Por último, respecto de los tipos penales que podrían ser aplicables a la intromisión en la correspondencia electrónica hay un elemento que no se examinará sino al final (3.4), dada su relevancia común para todos ellos: la falta de autorización o de voluntad del titular de la información privada –las comunicaciones o datos– para que el agente acceda a la información privada.

(3.1.) Intervención y difusión de comunicaciones privadas, del artículo 161-A del CP

Más arriba se anticipó que uno de los contextos o circunstancias en que se brinda protección penal a las comunicaciones y documentos –o hechos_ privados se da cuando se encuentran o se producen dentro de recintos o lugares que no están abiertos al público y son, además, en otro sentido, "privados".

Ese contexto y circunstancias son precisamente los señalados por el artículo 161-A del CP[24], que protege, según la doctrina, la intimidad de las personas[25] o la inviolabilidad de la vida privada[26].

---

24 Que, en lo que aquí interesa, sanciona al que: "[…] *en recintos particulares o lugares que no sean de libre acceso al público, sin autorización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado; […] o reproduzca documentos o instrumentos de carácter privado […]. Igual pena se aplicará a quien difunda las conversaciones, comunicaciones, documentos, instrumentos […] a que se refiere el inciso anterior*"

25 Díaz Tolosa, Regina (2007). "Delitos que vulneran la Intimidad de las Personas: Análisis crítico del artículo 161-A del Código Penal Chileno", *Ius et Praxis*, versión On-line, véase 13 n° 1, s/n° de pág. Disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122007000100011 [fecha de visita: 21 de noviembre de 2015]

26 Etcheberry (1998) 274.

Si se examina únicamente las conductas prohibidas, la intromisión del empleador en los correos electrónicos de un trabajador a lo menos realiza la hipótesis consistente en "captar", "interceptar" o "grabar" comunicaciones de carácter privado.

Sin embargo, una modalidad típica de lugar no se presenta en la conducta realizada por los empleadores.

En efecto, el carácter privado de las comunicaciones, conversaciones, documentos o hechos a que se refiere la disposición, a diferencia de los demás delitos que se examinan en este trabajo, no deriva de que cuenten con un soporte o continente que impide la percepción directa –exigencia que no aparece en el tipo penal–, sino, en primer lugar, de la circunstancia que el titular les haya confinado a ese "recinto" o "lugar"[27], excluyendo el acceso de terceros no autorizados[28] y, en segundo lugar, de que sean "privados"[29]. Y el caso es que ya la primera exigencia no se verifica en la intromisión del empleador en los correos electrónicos de sus trabajadores, que no tiene lugar en un "recinto" o "lugar" de acceso restringido, sino que consiste en una comunicación sostenida a través de un medio virtual, cuya protección contra el acceso no autorizado ciertamente puede afirmarse, pero no es (ni puede ser) relativa a un determinado "espacio": pues el correo electrónico, por definición, primero viaja por el espacio –en forma de señal o impulso electromagnético– antes de alojarse en un sistema de tratamiento de información y de ser recuperado ("bajado") en un dispositivo electrónico, que incluso puede ser portátil[30].

---

27 Explícitos en el sentido de que en este precepto la protección se circunscribe espacialmente, Medina (2008) 254 ("lugares especialmente protegidos"); y,; y Bascuñán Rodríguez (2014) 63 ("un espacio delimitado", añadiendo que, por criticable que sea esa decisión de política legislativa, es "indesmentible como premisa de la interpretación de ese precepto").

28 Bascuñán Rodríguez (2014) 63; Etcheberry (1998) 275; Matus, Jean Pierre y Ramírez, Mª Cecilia (2014). *Lecciones de Derecho Penal Chileno, Parte Especial*. 3ª edición. Santiago: LegalPublishing-Thomson Reuters. Tomo I, pp. 297.

29 El sentido de esta segunda nota de "privacidad" exigida por el tipo es discutido en doctrina, asimilándosela, por un sector, a la circunstancia de que los hechos o comunicaciones se refieran a la esfera "íntima" de la persona, como sostienen Matus/Ramírez (2014) 296, así como Garrido, Mario (2010) *Derecho Penal, Parte Especial*. 4ª edición. Santiago: Editorial Jurídica de Chile. Tomo III, p. 438, mientras que otra doctrina entiende que se agota en la circunstancia de que las "condiciones pragmáticas en que tiene lugar o se encuentra el objeto de ataque" (el hecho, conversación, comunicación o documento) dan cuenta de la voluntad de excluir a otros (lo que viene sugerido por el recinto en que tiene lugar o se encuentra, pero no depende únicamente de ello), como sostiene Bascuñán Rodríguez (2014) 63-64. En este lugar no es necesario tomar postura, pues de todos modos, como se verá a continuación (en el texto principal), en la intromisión del empleador en los correos electrónicos de los trabajadores falta ya la primera nota de privacidad exigida por el tipo.

30 Véase, al respecto, *infra* 3.3.

(3.2.) Apertura o registro de la correspondencia o de los papeles de otro

El artículo 146 tipifica y sanciona la conducta de *"[e]l que abriere o registrare la correspondencia o los papeles de otro"*. La doctrina, al parecer mayoritaria, entiende que la acción de "abrir" se refiere a la correspondencia; y la de "registrar", a los "papeles" (documentos)[31]. A continuación se examina, de forma separada, ambas modalidades, para luego hacer referencia sintética a un elemento común a ellas: la calificación fundada en la divulgación de secretos descubiertos a través de cualquiera de tales conductas.

(3.2.1.) Primera modalidad: apertura de correspondencia

El concepto de correspondencia se interpreta muy mayoritariamente como una comunicación efectuada a través de un medio "material" y "transmisible", cuyo contenido sea "aparente"[32]. La restricción estaría asociada a la interpretación del verbo rector "abrir", que supone un objeto "cerrado", sea por estar contenido en un sobre u otro continente similar, sea por estar doblado sobre sí mismo[33].

Esa interpretación del objeto material de la acción no parece dejar lugar al correo electrónico. Para ello, se opta por una comprensión, al parecer, naturalista de la voz "abrir", por sobre una comprensión normativa, concluyéndose que los paquetes de datos que son portadores de un mensaje electrónico ya son necesariamente "abiertos" y descifrados por el sistema de servicios de Internet, antes de ser retransmitidos al destinatario[34].

Como se ve, la restricción del alcance del tipo del artículo 146 del CP no tiene nada que ver con el significado del vocablo "correspondencia", cuyo sentido natural y obvio bien puede abarcar también a los correos electrónicos[35], sino con el sentido del verbo "abrir", que se entiende referido a correspondencia "cerrada". Sin embargo, si el sentido de la exigencia de un "cierre" es la expresión de una voluntad de exclusión, la "apertura" automatizada de los paquetes de datos efectuada por "el sis-

---

31 Etcheberry (1998) 266; Matus/Ramírez (2014) 289.

32 Etcheberry (1998) 266; Matus/Ramírez (2014) 289. Similar, Garrido (2010) 418. Así, también, Medina (2008) 250, refiriendo la exigencia de materialidad de la intromisión también a los papeles.

33 Etcheberry (1998) 266-267; Matus/Ramírez (2014) 289-290.

34 Matus/Ramírez (2014) 299.

35 Incluso mediante el discutible recurso al Diccionario de la Real Academia de la Lengua Española (en adelante, "el Diccionario"), no habría problemas, en la medida que este entiende como sinónimo de "correspondencia" al "correo", noción que a su vez, en una de sus acepciones, comprende expresamente al "correo electrónico".

tema" no constituye todavía aquella apertura intencional –efectuada por una persona– a la que el delito de inviolabilidad de las comunicaciones privadas quiere oponerse. Ese correo electrónico, ya alojado en el servidor, con indicación de un destinatario y de un "asunto", no leído aun por nadie, sigue sin ser "abierto", es decir, sin ser desplegado en la pantalla de un dispositivo –computador, teléfono móvil u otro– (o sin ser impreso), de modo que, entendiendo normativamente –en su sentido jurídico– el concepto de "apertura" no autorizada, no parece haber dificultades semánticas –es decir, derivadas del "sentido" de la ley– para entender que recién será abierto cuando alguien efectúe esa operación intencional.

Por su parte, el carácter "transmisible" del objeto material de la acción, asociado por la doctrina recién reseñada a la necesidad de que sea aparente, tampoco se opone a la inclusión de un correo electrónico como objeto de la acción. Si "aparente", en este contexto, quiere decir "que aparece y se muestra a la vista",[36] ello también puede decirse de los signos que resultan de la decodificación de los paquetes de datos en que consiste un correo electrónico cuando se le "abre"; y ciertamente se trata, además, de un objeto transmisible.

Esas consideraciones podrían bastar, si se atiende al tenor literal y al argumento teleológico –referido a la finalidad de protección de la inviolabilidad de las comunicaciones privadas– para admitir al correo electrónico como objeto de protección del tipo penal de violación de correspondencia, del artículo 146 del CP. Así lo entiende alguna doctrina, al parecer, más bien aislada[37, 38].

Sin embargo, a favor de entender excluida del ámbito del artículo 146 del CP la apertura de correspondencia electrónica, más allá de las razones basadas en su tenor literal, invocadas por una doctrina mayoritaria –si esta expresión puede usarse en un contexto de tratamiento más bien fragmentario de la cuestión por la literatura nacional–, también se ha esgrimido un argumento sistemático. Conforme a este argumento, implícitamente sugerido por los autores antes mencionados, el correo electrónico no estaría protegido por el artículo 146 del CP, sino que encontraría su protección penal, y de forma similar a la de las cartas (entendiendo a la "correspondencia" como referida únicamente a "cartas" escritas en papel u

36 La única acepción que viene al caso, de las que registra el Diccionario.

37 Moscoso, Romina (2014). "La Ley 19.223 en general y el delito de hacking en particular". *Revista Chilena de Derecho y Tecnología*, Vol 3 N° 1, pp. 11-78, p. 52.

38 Tampoco tiene problemas para entender que los correos electrónicos son "correspondencia" –en el sentido de esa disposición– una decisión de la Corte de Apelaciones de Valparaíso que, si bien recayó en una causa no penal, explícitamente se refirió al artículo 146 del CP; véase Corte de Apelaciones de Valparaíso. 22 de octubre de 2010. Rol N° 504-2010. No disponible en colecciones físicas o electrónicas.

otro soporte semejante), en otras disposiciones penales –el artículo 36 B, letras c) y d) de la Ley Nº 18.168 y, en su caso, el artículo 2º de la Ley de Delitos Informáticos–[39].

Pero, aun teniendo en cuenta estas otras disposiciones, si se ha descartado una incompatibilidad semántica entre el concepto de "apertura de correspondencia" y la hipótesis de intromisión en los correos electrónicos, ¿no cabe la alternativa de afirmar, más bien, que también es aplicable, *prima facie*, el artículo 146 del CP, y que, sin embargo, estamos ante un concurso aparente de leyes penales que, resuelto por subsidiariedad[40], termina desplazando a la norma del artículo 146 del CP? La magnitud de las penas por el acceso o captación no autorizados de los datos informáticos o señales electromagnéticas, muy semejantes a las de la apertura de correspondencia, pero ligeramente exasperadas, sugeriría sin problemas esta solución. Y la preferencia por estas figuras se explicaría porque captarían las intromisiones en correos electrónicos ajenos con mayor especificidad, esto es, asignando relevancia al hecho de que la comunicación tiene lugar a través de servicios públicos de telecomunicaciones, o que la comunicación quedó alojada en un sistema de tratamiento de información.

Bajo esta interpretación, si, atendida la configuración específica de los tipos de la Ley de Telecomunicaciones, ellos dejasen una "laguna" sin punir, respecto de una conducta que, en cambio, sin dificultad puede ser entendida como "apertura de correspondencia" (electrónica), entonces no habría razón para dejar de aplicar el tipo del artículo 146 del CP –como norma subsidiaria– a tal comportamiento, con una pena semejante –en su caso, ligeramente inferior– a la de aquellas leyes penales especiales[41].

---

39 Etcheberry (1998) 267. Similar, Matus/Ramírez (2014) 300-301, afirmando que: "puesto que ellos no existen físicamente como las cartas […] no parece, *prima facie*, que las disposiciones de los artículos 146 […] sean aplicables a supuestos de acceso no autorizado a los servidores donde se encuentran registrados [los correos electrónicos] o a las líneas de comunicación a través de las cuales se transmiten. En el primer caso, el art. 2º de la Ley Nº 19.233 […] parece ofrecer una razonable descripción del hecho, imponiendo una pena que no se aleja significativamente de las previstas en las disposiciones del Código antes referidas […]. Respecto de la interceptación de la transmisión de los correos […] las disposiciones aplicables parecen ser, con propiedad, las de las ya mencionadas letras b) y c) del art. 36 B, letra c) de la Ley General de Telecomunicaciones"

40 Sobre el sentido y el ámbito de aplicación de los principios llamados a resolver los concursos de normas, sintéticamente, Couso, Jaime (2011b), "Comentario a previo los Arts. 74 y 75", en Couso/Hernández, *Código Penal Comentado, Parte General*, Abeledo Perrot - LegalPublishing, Santiago, pp. 655 y ss.

41 Tal sería el caso si se entiende que la interceptación "maliciosa" de una señal que se emita a través de un servicio público de telecomunicaciones no abarca las conductas ejecutadas con dolo eventual (véase *infra*, 3.3.2.) y se admite, en cambio, esa forma de dolo como suficiente para realizar el tipo del artículo 146 del CP (la doctrina nacional no se refiere a una exigencia de dolo directo en esta figura, lo que debe ser entendido en el sentido de que se conforma con dolo eventual, máxime si –ofreciendo con ello un argumento *a contrario*– se

Asimismo, si en el futuro una modificación legal a los tipos de la Ley de Telecomunicaciones tuviere por efecto que deje der ser subsumible en ellos una hipótesis de captación de correo electrónico (por ejemplo, si se introdujere una exigencia típica de perjuicio) que, sin embargo, califica como apertura de correspondencia (electrónica), también cabría sancionar por la mera apertura de correspondencia.

Contra la tesis del concurso aparente de leyes penales podría sostenerse que, aun si el concepto de "apertura de correspondencia" pudiese abarcar semánticamente la intromisión en correos electrónicos, esta hipótesis quedaría fuera del alcance del tipo penal del artículo 146 del CP más bien por una cuestión de delimitación sistemática entre tipos penales que tienen capacidad de rendimiento similar para la protección de las comunicaciones privadas, pero que "se dividen el trabajo", abarcando, uno de ellos, la protección de la privacidad de las cartas, y el otro, la de los mensajes enviados a través de telecomunicaciones o almacenados en sistemas de tratamiento de información. En ese sentido, los "nuevos" tipos introducidos posteriormente por leyes especiales habrían venido a acotar, por contraste, el concepto legal de "apertura de correspondencia", que (ya) no se entendería referido a la correspondencia electrónica, a la que el legislador precisamente quiso proteger en otro lugar. En tal caso, el alcance de la protección a los correos electrónicos estaría circunscrito a los términos –más o menos estrictos– de estos nuevos tipos penales, y su suerte futura está atada a la de ellos, en el sentido de que cualquier "laguna" de punibilidad que sea identificada en la regulación vigente (apertura con dolo eventual) o que surja de una reforma futura (en el ejemplo propuesto, apertura sin irrogación de un perjuicio), ya no dejaría a salvo la posibilidad de recurrir, de forma subsidiaria, al artículo 146 del CP.

La disyuntiva tiene, como se ve, cierta relevancia. La cuestión se ha planteado en el derecho comparado, pero es interesante hacer notar que, para las hipótesis tenidas en cuenta en este trabajo, nunca ha estado en juego el resultado fundamental de que los correos electrónicos están protegidos penalmente. En efecto, sea porque al momento en que se masificó su uso sencillamente se les entendió como "correspondencia" y quedaron por ello cubiertos por los tipos tradicionales de apertura de cartas, sea porque, antes de su masificación, se crearon tipos penales específicos para

es explícito en exigir dolo directo solo para la violación de correspondencia ejecutada por un funcionario público; véase así, Garrido (2010) 420): entonces, la apertura de un correo electrónico, con dolo eventual (por ejemplo, sin certeza de que está dirigido exclusivamente a un tercero, pero con indiferencia frente a esa posibilidad), realizaría el tipo penal del artículo 146 del CP, pero no el de la Ley de Telecomunicaciones.

proteger a los correos electrónicos, estos parecen haber gozado siempre de una protección relaticamente simétrica a la de las cartas[42].

Panorama comparado: correlación entre una interpretación restrictiva del objeto de la violación de correspondencia y la existencia de protección relativamente simétrica para los correos electrónicos.

Tres casos de derecho comparado permiten iluminar la situación del derecho chileno, tanto para resolver la relación entre los tipos del Art. 146 del CP y los de las leyes especiales en materia de telecomunicaciones y delitos informáticos –en caso de que se consideren estos aplicables–, como para abonar la conclusión de que, si estos no se considerasen aplicables a los correos electrónicos, la apertura de correspondencia del Art. 146 sí debería serlo.

El primer caso es el del derecho penal español, que puede ser caracterizado como uno en que la simetría en la protección es completa, y explícita, de modo que no tiene ningún sentido –y con ello, deja de ser semánticamente posible– incluir el concepto de "correo electrónico" dentro del de "carta".

En efecto, la voluntad del legislador español de brindar protección simétrica a las comunicaciones y documentos en uno y otro tipo de soporte se tradujo lisa y llanamente en que decidió tipificar en una única y misma disposición, de modo completamente equivalente, la intromisión en ambos tipos de comunicación. En efecto, el artículo 197.1 del CP español[43] castiga con penas de prisión y multa al 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".*

---

42 "Relativamente simétrica" quiere decir aquí que, en diversos preceptos o en uno mismo que alude alternativa y diferenciadamente a ambos objetos, se protege la privacidad o inviolabilidad tanto de las cartas como de los correos electrónicos. No supone, en cambio, que las penas sean exactamente las mismas, ni que las modalidades (y figuras calificadas, en su caso) coincidan en todo. De hecho, ello no es así en varios de los países que han legislado en la materia (véase *infra*, el apartado siguiente, en el texto principal). Pues las reformas legales con frecuencia han estado presididas por un propósito de reforzar la protección de los medios electrónicos; y, en ocasiones, han adaptado las modalidades ejecutivas a la especial naturaleza de tales soportes. V., sin embargo, Londoño, Fernando (2004) "Los Delitos Informáticos en el Proyecto de Reforma en Actual Trámite Parlamentario", *Revista de Derecho Informático*, Nº 4, mayo de 2004, pp. 171-190, 176, favorable a la igualación de penas –que de hecho venía propuesta por la reforma examinada– entre la apertura de cartas y registro de correspondencia, por una parte, y el acceso indebido al contenido de un sistema de tratamiento de información, por la otra.

43 En general, sobre la disposición y su ámbito de aplicación, véase Muñoz Conde, Francisco (2015). *Derecho Penal, Parte Especial.* 20ª edición. Valencia: Tirant lo Blanch, pp. 233 y ss.

Esa decisión, muy temprana, en términos relativos (en 1995, cuando apenas comenzaba a utilizarse el correo electrónico), evitó toda necesidad de preguntarse si el correo electrónico calificaba como carta o "papeles". De hecho, un año antes, en 1994, el anterior CP ya había incluido junto al delito de descubrimiento y relevación de secretos del artículo 497 –que se refería solo al apoderamiento de cartas o papeles de otro–, en un nuevo artículo 497 bis, un delito de similar tenor (descubrimiento de los secretos) pero referido a la "interceptación de telecomunicaciones"[44]. El nuevo CP de 1995 unificó ambas conductas, explicitando que los correos electrónicos eran un objeto protegido.

Es obvio, entonces, que el sentido de la palabra "carta" en el artículo 197.1 del CP español viene determinado –restrictivamente– por la protección simétrica que reciben los correos electrónicos en la misma disposición. Los correos electrónicos no son una especie del género "cartas", sino un objeto distinto de estas. La "prueba" patente de ello es que el correo electrónico tiene protección paralela, en el mismo precepto, junto a (y no "dentro de") la protección brindada a las cartas. Y si no existiese esa mención, que hace explícita la protección al correo electrónico, habría una (importante) razón menos a favor de una interpretación restrictiva de la "carta", que pretendiese dejar a aquel fuera del contenido semántico de la voz esta.

El segundo caso es el del derecho alemán, y se caracteriza también por la introducción, bastante temprana, de una protección relativamente simétrica (aunque no completamente, como en el caso español) entre la protección de la privacidad de las "cartas" y la de los correos electrónicos.

En efecto, el concepto de carta (*Brief*), en el § 202 del CP alemán, se entiende de modo restringido, por la doctrina, abarcando solo aquellos escritos (*Schriftstücke*), con un contenido ideológico, cuyo soporte sea material y se encuentre cerrado[45]. Ello no incluye a los correos electrónicos. Determinante de esta interpretación restrictiva es el hecho de que muy temprano, en 1986, antes de que el correo electrónico llegase a emplearse como medio de comunicación, una reforma legal había incorporado un tipo penal específico para la intromisión en datos electrónicos, el § 202a del CP, que permitía sancionar la apertura no au-

44 Véase el tenor de ambas disposiciones en http://noticias.juridicas.com/base_datos/Penal/d3096-1973.html#a497 [fecha de visita: el 25 de noviembre de 2015].

45 Kargl (2013). "§ 202 StGB". En Kindhäuser, Urs / Neumann, Ulfried / Paeffgen, Hans-Ulrich (Editores), *NomosKommentar, Strafgesetzbuch*. 4ª edición. Baden-Baden: Nomos. Vol. II, § 202, nm 3 y ss.

torizada correos electrónicos sin necesidad de recurrir al § 202[46]. Esta interpretación viene abonada por el hecho de que el propio § 202, que castiga la apertura de cartas, antes de la reforma de 1986 contaba con un párrafo tercero que había sido introducido unos años antes para ampliar la protección penal a otro tipo de soportes de la comunicación de ideas, distintos de la "carta" en sentido estricto. Pero justamente en 1986, con la introducción del § 202a, que ahora sancionaba expresamente la intromisión en datos electrónicos, el § 202 fue modificado para (volver a) referirlo únicamente a escritos (e ilustraciones) en soporte físico, de modo de evitar que se solapase con el nuevo parágrafo referido a datos electrónicos[47]. Finalmente, la introducción, en 2007, de un nuevo tipo penal –en el § 202b– que sanciona la captura de datos mientras son transmitidos por un medio que no es de acceso público, complementa la protección de los correos electrónicos, volviéndola bastante simétrica con la brindada por el § 202 a las cartas[48] [49].

El tercer caso es el del Derecho austríaco.

Lo peculiar del caso de Austria es que estableció tipos penales especiales para la protección de los correos electrónicos ya bastante años después de que los correos electrónicos comenzaran a usarse masivamente, lo que hizo necesario preguntarse, antes de esa reforma, cuál era el estatuto penal de las intromisiones en los correos electrónicos. En efecto, recién en el año 2002 Austria estableció los tipos penales de acceso no autorizado a un sistema informático (§ 118a del CP) y de afectación del secreto de las telecomunicaciones (§ 119 del CP), en cumplimiento de lo dispuesto por el Convenio sobre Ciberdelincuencia del año 2001 (Convenio de Budapest), que ese país había suscrito un año antes y ratificó ese mismo año.

---

46 La explicación es de Hoeren, Thomas (2001). "Briefgeheimnis im Strafrecht und E-Mail in Ö und D, Ein Microvergleich". *Universitätslehrgang für Informationsrecht und Rechtsinformation - Rechtswissenschaftliche Fakultät Wien* Viena: Max W. Mosin. Disponible en http://www.it-law.at/wp-content/uploads/2014/09/mosing-hoeren1.pdf [fecha de visita: 18 de noviembre de 2015], p. 8, en un artículo que compara el ámbito de los tipos penales de apertura no autorizada de cartas en el derecho penal austríaco y el alemán.

47 Kargl (2013) § 202, número marginal 1.

48 Kargl (2013) § 202b, nm 1 y ss.

49 El hecho de que las penas para la intromisión en datos electrónicos (en los §§ 202a y 202b) sean superiores a la contemplada por el § 202 para la apertura (o intromisión en el contenido) de cartas, si bien relativiza (cuantitativamente) la tesis de la protección simétrica, no afecta la validez del argumento sistemático que se ha sostenido más arriba (la interpretación restrictiva del concepto de "carta" es correlativa a una protección relativamente simétrica –en este caso, por medio de disposiciones paralelas– para cartas y correos electrónicos); al contrario, en siento sentido la refuerza: si en el derecho alemán no se aplica a los correos electrónicos la protección bridada a las "cartas", ello no se debe a que semánticamente este concepto no sea capaz de abarcar a aquellos, sino al hecho de que, cuando comenzaron a ser utilizados como un medio de comunicación, ya contaban con un precepto que permitía brindarles una protección penal, no idéntica, sino incluso reforzada.

Hasta entonces, el único tipo penal disponible para proteger la privacidad de los correos electrónicos en Austria era justamente el de apertura de cartas cerradas (§ 118 del CP).

Ello explica que hasta el año 2001, un sector relevante de la doctrina no haya tenido problemas en considerar incluidos, dentro del ámbito de los objetos protegidos por el § 118a, a los correos electrónicos[50]. Así, según Hoeren[51], si las notas penalmente relevantes de la noción de "carta", son que consista en un escrito, fundamentalmente a base de letras o números, con un contenido ideológico o conceptual perdurable, y que cuente con un remitente y un destinatario, todas esas notas son predicables de un correo electrónico. En particular:

> *"Si se compara esa definición con el proceso técnico que tiene lugar respecto de los e-mails puede apreciarse que, a través de la descarga de los e-mails es posible hacer legible para el receptor un contenido ideológico. Este contenido es transmitido a través de letras. También la exigencia de perdurabilidad se da del mismo modo que para una carta en sentido tradicional: esta se abre y, tras la lectura es, ora conservada, ora desechada. El e-mail es recuperado en la pantalla, leído y luego, o bien eliminado, o bien archivado en forma de un impreso o de un dispositivo de almacenamiento"*[52].

Y, en particular, la exigencia de que la carta esté protegida por una "cubierta", que impida acceder directamente a ella, sin "abrirla", es decir, sin romper una barrera de protección ideal (ideal, porque no importa por la dificultad material que opone), también se aprecia sin problemas en un correo electrónico:

> *"[e]l e-mail es producido con una "cubierta electrónica". Ella no está hecha de un sobre protector de carácter físico y no puede por ello ser abierto de forma mecánica. Pero sería muy restrictivo exigir una afectación sustancial de esa especie para el concepto de "abrir". El § 118 del CP designa como objeto la "carta cerrada". Esta exigencia es satisfecha por un e-mail con código seguro. Para un e-mail cerrado no es nece-*

50 Así lo sostenían entonces dos de los principales comentarios al CP austríaco (Leukaf/Steiniger, *Kommentar zum Strafgesetzbuch*, 3ª edición, par. 118, número marginal 4; y Meyerhofer/Rieder, *Das österreichische Strafrecht, I Teil, Strafgesetzbuch*, 4ª edición, vol. XI, par. 118, número marginal 13), citados por Hoeren (2001) 4. En contra, en cambio, Wessely (1996), "Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet". ÖIZ, p. 612, citado por Hoeren (2001) p. 4.

51 Hoeren (2001) 3.

52 Hoeren (2001) 3.

sario que esté en clave. Del mismo modo que para el envoltorio de un mensaje no se exige un blindaje, tampoco me parece que pueda exigirse, para cumplir con la exigencia de "cierre" del e-mail, que se encuentre en clave"[53].

Ahora bien, tras la introducción en el CP austríaco de tipos penales destinados especialmente a proteger la confidencialidad del contenido de los sistemas informáticos y el secreto de las telecomunicaciones, la doctrina parece entender, casi sin matices, que el concepto de "carta", del § 118 ya no puede referirse a los correos electrónicos[54].

Esta evolución de la interpretación del concepto de carta, y del alcance del tipo común de violación de correspondencia, en el Derecho austríaco, da cuenta clara, de nuevo, de la correlación entre una protección simétrica explícita entre cartas y correos electrónicos y una restricción del primer concepto.

¿En qué situación se encuentra el Derecho chileno, en comparación con la de esos otros ordenamientos jurídicos?

En mi opinión, como se verá al revisar el artículo 36 B, letras c) y d), de la Ley de Telecomunicaciones y los artículos 2° y 4° de la Ley de Delitos Informáticos, su relación con el Art. 146 del CP es –en términos relativos– similar a la que en el Derecho alemán se da entre la protección de la privacidad de los datos (en este caso interesan los correos electrónicos) y la protección de la inviolabilidad de las cartas: aquellas disposiciones de la Ley de Telecomunicaciones y la Ley de Delitos Informáticos ofrecen a la privacidad de las comunicaciones (y documentos) electrónicas, desde antes de la masificación de los correos electrónicos, una protección relativamente simétrica con la que ofrece el artículo 146 a la "correspondencia", de modo que sistemáticamente es lógico asumir una "división del trabajo", conforme a la cual esta última disposición se debe entender referida únicamente a la correspondencia con soporte físico.

Pero, para insistir una vez más en que el argumento sistemático es determinante, si se concluyese que, en realidad, ni el artículo 36 B, letras

53 Hoeren (2001) 4. En realidad, como aclara el autor, la "cubierta cerrada" de los e-mails se presenta de dos modos diversos, según si está siendo transmitido o si está almacenado en el computador del remitente o en el del receptor. En el primer caso, la "cubierta cerrada" consiste en diversos "paquetes" de datos, cuya lectura no es posible sin su decodificación, mediante la "apertura" del e-mail, que reúne los diversos paquetes de datos y convierte estos en símbolos legibles; en el segundo caso, la "cubierta cerrada" puede consistir en algo distinto: en el almacenamiento de los e-mails en una cuenta a la que no se accede sin ingresar la clave (y el nombre de usuario). En ambos casos se estaría ante una carta cerrada en el sentido del § 118 del CP austríaco (pp. 4-5).

54 Por todos, Lewisch, Peter (2008). "§ 118 StGB". *Wiener Kommentar zum Strafgesetzbuch*. 2ª edición. Viena: Manz Verlag, § 118, nm 5.

c) y d), de la Ley de Telecomunicaciones, ni los artículos 2º y 4° de la Ley de Delitos Informáticos se refieren a correos electrónicos, el delito de apertura de correspondencia (y el de registro de papeles, como se verá) del artículo 146 del CP, sin ninguna dificultad semántica debería entenderse referido también a la apertura (o registro) de los correos electrónicos. Si en Austria, antes de la reforma de 2002, un contexto sistemático similar a ese –ausencia de tipos especialmente referidos a comunicaciones electrónicas– dio lugar a una doctrina relevante en tal sentido, aun sobre la base del concepto legal de "cartas", con mayor razón ello sería posible en Chile a partir de un concepto legal aun más amplio, como el de "correspondencia". El tenor literal no se opondría a ello –salvo con una interpretación naturalista del concepto "abrir"–, la interpretación teleológica lo favorecería, y la interpretación sistemática en tal caso no exigiría restricción alguna, pues no habría disposiciones en leyes especiales cuya referencia a los correos electrónicos clarificase, por contraste, la situación de estos en relación con el artículo 146 del CP.

(3.2.2.) Segunda modalidad: registro de papeles

Por lo que atañe a la segunda modalidad típica del artículo 146 del CP, el registro de los "papeles" de otro, la doctrina mayoritaria no tiene problemas, esta vez, en normativizar el concepto, abarcando el registro de cualquier "documento", y entendiendo que los documentos pueden consistir en registros magnéticos, como el de una cinta magnetofónica[55]. Esta normativización del concepto permite perfectamente entender abarcado, dentro de la figura de "registro no autorizado de papeles", precisamente el registro de correos electrónicos o de documentos adjuntos a ellos.

Con todo, y de modo semejante al caso de la interpretación del concepto "correspondencia", en relación con la pregunta de si abarcaba a los correos electrónicos, las dudas pueden venir planteadas por una interpretación sistemática del alcance de la noción "papeles", desde el momento en que se sugiere, por la misma doctrina que normativiza este concepto,

55 Así, Etcheberry (1998) 268, sugiriendo que en el caso de los papeles, a diferencia del de las cartas, no se exige materialidad (si bien la doble negación confunde). Matus/Ramírez (2014) 289, también entiende "papeles" en el sentido de "documentos", es decir, "en general, manifestaciones de pensamiento fijadas en un medio transmisible y que no sean de conocimiento público", al parecer sin restricciones sobre el soporte –en la medida que sea uno que permite la transmisión–. Por su parte, Garrido (2010) 422, entiende que los papeles son "documentos privados […] de cualquier naturaleza", pero sin referirse expresamente a si ello exige o no materialidad, aunque por contraste con la exigencias dirigidas a la correspondencia, la afirmación de que los documentos pueden ser "de cualquier naturaleza" puede entenderse en un sentido similar a la apertura conceptual admitida por los demás autores mencionados.

que para los documentos en soporte electrónico –o electromagnético– la legislación penal ha introducido, en el artículo 2º (y 4°) de la Ley de Delitos Informáticos, un tipo penal que ofrece una protección "simétrica" a la que el artículo 146 brinda a la privacidad de los "papeles", como se desprende del siguiente planteamiento de Etcheberry:

> *"El artículo 146, como hemos visto, sanciona a quien abre o registra los papeles de otro, regulación que a la época en la cual se promulgó cubría las intromisiones en la esfera de la intimidad de los sujetos. El progresivo desarrollo de la tecnología ha puesto hoy a la informática o computación al servicio de los más vastos asuntos, al punto de que los "papeles" van siendo desplazados por la tecnología de almacenamiento digital […] El articulado del La Ley 19.223 contiene tanto figuras de destrucción como de mera intromisión […] [sancionándose en su artículo 2º] el mero conocimiento, para lo cual es necesario que preceda el registro previo"*[56].

Es decir, y esta vez ya sin problemas derivados de una comprensión naturalista del tenor literal del objeto de la acción –pues los "papeles" claramente se entienden en sentido normativo–, una restricción del alcance de la figura típica, para excluir el registro de correos electrónicos y de sus documentos adjuntos, solo tiene sentido si resulta clara la existencia de una "división del trabajo" entre dos tipos penales, que aseguren una protección relativamente simétrica a la privacidad de los documentos, en formato electrónico –en los artículos 2° y 4° de la Ley de Delitos Informáticos– y en formato físico –en el artículo 146 del CP–.

Y, en mi opinión, como se verá más abajo, la protección de los datos electrónicos que resulta de los artículos 2° y 4° de la Ley de Delitos Informáticos efectivamente es, salvadas las diferencias por la naturaleza del soporte, relativamente simétrica con la que el artículo 146 del CP brinda a los "papeles". Por ello, hay buenas razones para sostener, también respecto de esta modalidad, una "división del trabajo", que semánticamente hace innecesario entender abarcados los documentos electrónicos dentro del concepto normativo de "papeles".

(3.2.3.) Calificación por la divulgación de los secretos descubiertos

Por último, respecto de ambas modalidades, es necesario tener en cuenta que el artículo 146 distingue entre una figura básica y una cali-

56 Etcheberry (1998) 271.

ficada, señalando penas distintas en cada caso. La calificación exige, en primer lugar, que la correspondencia contenga algún "secreto", es decir, en palabras de Etcheberry, "un hecho que es conocido solo en un círculo restringido de personas y respecto del cual existe, por parte de alguien, un interés legítimo en que el conocimiento se mantenga limitado a ese círculo de personas, pues su conocimiento por otros afectaría adversamente a un bien de que es titular (su honor, sus intereses, su tranquilidad, etc.)"[57]. Y, en segundo lugar, exige que ese secreto haya sido "divulgado" a terceros, bastando para ello con "la revelación a una sola persona"[58]. La falta de cualquiera de esas dos circunstancias –no había secretos en la correspondencia, o no fueron divulgados–[59] lleva a la aplicación solo de la figura básica.

(3.3.) Captación y difusión de comunicaciones sostenidas a través de servicios públicos de telecomunicaciones, y acceso no autorizado y revelación de datos de un sistema de tratamiento de información

Los delitos que se examina a continuación tienen como objeto específico de protección comunicaciones o datos con soporte "técnico". En el caso de las comunicaciones, el soporte son señales de telecomunicaciones, que se transmiten en base a "líneas o redes de telecomunicaciones mediante impulsos eléctricos"[60]. En el caso de los datos, el soporte son diversos medios de almacenamiento, sean semiconductores, magnéticos u ópticos[61].

Antes de examinar los tipos, en particular, es necesaria una breve explicación sobre el modo en que operan los correos electrónicos, sea como forma de comunicación, sea como datos que pueden ser almacenados.

---

57 Etcheberry (1998) 269.

58 Etcheberry (1998) 269; similar Matus/Ramírez (2014) 290.

59 Etcheberry (1998) 268-269, expresamente dando por configurada la figura básica, si la correspondencia no contenía secretos.

60 Así se definió el objeto de protección, durante la tramitación de la Ley de Telecomunicaciones; véase Primer Informe, Comisión de Transportes y Telecomunicaciones de la Cámara de Diputados, de 14 de septiembre de 1992, Boletín 400-15.

61 Veáse, la voz "computer data storage" en en.wikipedia.org. Disponible en https://en.wikipedia.org/wiki/Computer_data_storage#Storage_Media [fecha de visita: 30 de noviembre de 2015]. Por su parte, los medios de almacenamiento basados en papel perforado ya no parecen estar en uso, pero nada se opone a su inclusión como soporte de un sistema automatizado de tratamiento de información.

(3.3.1.) Los correos electrónicos, su forma de operación y las alternativas para la intromisión en ellos

El correo electrónico es una herramienta de internet que permite enviar y recibir mensajes por medios electromagnéticos[62]. El recorrido de esos mensajes consiste en una red de computadores, a través de los cuales van viajando los paquetes de datos a partir de ciertas instrucciones efectuadas por los usuarios. En su recorrido más simple, el envío involucra a lo menos 4 computadores. El primer computador es el del remitente, que, a través de un programa de mensajería electrónica, redacta el mensaje, al que vienen asociados una fecha, el nombre del remitente y su dirección electrónica; una vez que el remitente da la instrucción de envío del mensaje, esa información viaja a otro computador, el del servidor de correo electrónico del remitente, que a su vez identifica –en la dirección de correo electrónico que el remitente señaló para el destinatario– cuál es el servidor que presta servicios al destinatario, y lo reenvía al mismo[63]. El servidor del destinatario recibe, en un tercer computador, el mensaje y, luego de identificar la dirección específica del destinatario y su capacidad para recibir otro mensaje, lo envía al mismo. Una vez que el destinatario descarga el mensaje, este se almacena en su computador, el cuarto de la cadena[64].

Una peculiaridad a tener en cuenta es que, mientras el servidor del remitente no logra enviar el mensaje al destinatario, el mensaje se almacena en ese servidor, que reintentará el envío tiempo después –unas horas más tarde, generalmente–. Recién tras su despacho exitoso, el mensaje es borrado del servidor del remitente. A su vez, mientras el destinatario no descarga el mensaje, este permanece almacenado en su servidor –el servidor del destinatario–[65].

Así, los correos electrónicos pueden verse en dos facetas. En primer lugar, como comunicaciones, que son transportadas por señales que responden a impulsos eléctricos, y que tienen lugar a través de servicios públicos de telecomunicaciones, cuya inviolabilidad está protegida penalmente[66]. En segundo lugar, pueden verse como datos almacenados en

62 Para las explicaciones que vienen a continuación, véase en general, Rodríguez, Eduardo (2003). "El correo electrónico". *Revista Chilena de Derecho Informático*, número 3. Disponible en: http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewArticle/10668/11414 [fecha de visita: 30 de noviembre de 2015], s/n° de página.

63 Rodríguez (2003) s/n° de pág.

64 Rodríguez (2003) s/n° de pág.

65 Rodríguez (2003) s/n° de pág.

66 Álvarez Valenzuela (2005) 201-202.

computadores, esto es, en un sistema de tratamiento de información, cuya confidencialidad también está protegida penalmente[67].

Cuál de esas facetas es la que está en juego en una determinada hipótesis fáctica, es algo que depende de la etapa en la que se encuentra el mensaje electrónico al momento de la conducta cuya tipicidad se examina.

Una mirada al derecho alemán, en el que estas dos facetas están claramente distinguidas, y son objeto de dos tipos penales diferentes, puede servir de aclaración, pues como se verá, el derecho chileno también puede ser interpretado a partir de la distinción entre ambas facetas de la protección de los datos.

En Alemania, en efecto, se entiende que los correos electrónicos pueden ser objeto de una intromisión penalmente relevante, tanto de la forma descrita por el § 202a del CP, que castiga el "espionaje de datos" –referido no solo al tráfico de las telecomunicaciones, sino principalmente a cualquier dato que pueda estar grabado en un computador y asegurado especialmente contra el acceso no autorizado–[68], como de la forma señalada por el § 202b del CP, que castiga el apoderamiento o captación de datos que están siendo objeto de una transferencia no pública de datos o de una transmisión electromagnética hecha por un equipo o planta de procesamiento de datos[69]. Y la línea divisoria está trazada justamente en la distinción entre un acceso a datos almacenados y uno a datos cuyo envío aún está en curso. Así, si el mensaje está ya almacenado en el computador del trabajador de una empresa, luego de que este lo "bajó" desde el servidor a su computador, el acceso no autorizado es típico del § 202a del CP, siempre que los datos estén especialmente asegurados contra tal acceso (exigencia típica expresa de esa disposición); en cambio, si el mensaje está almacenado en el servidor del remitente, de modo que el trabajador, con solo conectarse al servidor, aun puede bajarlo a su computador, teléfono o dispositivo móvil, entonces se entiende que aún está en proceso de transferencia de datos[70].

---

67 Véase, ya en 1991, en la Exposición de Motivos del Proyecto de Ley sobre Delito Informático (Boletín 412-07, de 16 de julio de 1991, Moción del Diputado José Antonio Viera. (Gallo), que los sistemas de tratamiento de información a los que alude el delito informático incluyen a las redes de computadores.

68 Por ejemplo, en el computador del trabajador.

69 Eisele, Jörg (2012). "Arbeitnehmerüberwachung und Compliance unter Berücksichtigung der Cybercrime-Konvention". *Zeitschrift für Internationale Strafrechtsdogmatik*, 2010, vol. 8-9/2012, pp. 402-408, 405.

70 Eisele (2012) 406.

Una delimitación similar puede efectuarse en el derecho penal chileno. Si el mensaje ya fue enviado, pero aún no recibido, porque aún se encuentra en el servidor del destinatario, lo que viene a cuento es examinar una posible afectación de la inviolabilidad de las comunicaciones privadas, realizadas por medio de un sistema público de telecomunicaciones, del artículo 36 B, letra c), de la Ley de Telecomunicaciones. Si el mensaje aún no ha sido enviado, o ya fue recibido por el destinatario, que lo descargó desde su servidor a su computador o dispositivo móvil, el acceso no autorizado a este computador o dispositivo, para conocer el mensaje, interesa como posible infracción a la confidencialidad de estos sistemas y de los datos contenidos en él, del artículo 2° de la Ley de Delitos Informáticos.

Hechas esas aclaraciones, ahora corresponde examinar los tipos de la Ley de Telecomunicaciones y de la Ley de Delitos informáticos para verificar si es subsumible en ellos la intromisión del empleador en los correos electrónicos del trabajador.

(3.3.2.) Captación y difusión de comunicaciones sostenidas a través de servicios públicos de telecomunicaciones, del artículo 36 B, letras c) y d), de la Ley de Telecomunicaciones

El artículo 36 B, letra c), de la Ley de Telecomunicaciones 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 público de telecomunicaciones".*

Por su parte, la letra d) del mismo artículo castiga:

> *"[l]a difusión pública o privada de cualquier comunicación obtenida con infracción a lo establecido en la letra precedente".*

La introducción de las letras c) y d) del artículo 36 B de la Ley de Telecomunicaciones, por la Comisión de Transportes y Telecomunicaciones de la Cámara de Diputados, durante la tramitación de la Ley Nº 19.277, pretendió, como la misma Comisión afirmó:

> *"sancionar en forma drástica la violación de las comunicaciones privadas, sin autorización del dueño […] Se viola la privacidad de las*

comunicaciones hechas a través de servicios públicos de telecomunicaciones, que no sean de libre recepción"[71].

Además, esta nueva forma de protección a las comunicaciones se entendió como complementaria de la brindada, en general, a las comunicaciones, por el Código Penal, razón por la cual se prefirió mantener el tipo en una ley especial[72].

Que el servicio de acceso a internet sea un servicio público de telecomunicaciones no parece estar en duda[73]; y siendo el correo electrónico una de las herramientas de internet, tampoco se duda sobre la protección penal del mismo bajo el artículo 36 B de la Ley de Telecomunicaciones, en general, y de sus letras c) y d), en particular[74].

Se trata, pues, de uno de los casos en que la expectativa de exclusión de terceros se desprende del hecho que la comunicación o el documento cuenta con un soporte o continente que impiden la percepción directa, como ocurre con la telefonía, el correo electrónico, la mensajería a través de teléfonos móviles, entre otras[75]. Su carácter "privado" se desprende del hecho que los intervinientes en la comunicación se dirigen a través de tales señales a destinatarios determinados, con exclusión de terceros. Así lo entiende la doctrina[76], y la jurisprudencia constitucional[77]. El impedimento a la percepción directa viene impuesto por el medio a través del

71 Primer Informe, Comisión de Transportes y Telecomunicaciones de la Cámara de Diputados, de 14 de septiembre de 1992, Boletín 400-15, s/n° de página. La Comisión pretendió "buscar un tipo penal para sancionar a aquel que tome conocimiento y difunda el secreto de una comunicación efectuada a través de un servicio público de telecomunicaciones que no sean de libre recepción y sin permiso de quien utiliza el servicio: telefónico, télex, transmisión de datos, etc. Para la historia fidedigna de la ley se dejó constancia que, técnicamente, la expresión "señal de telecomunicaciones" implica conversaciones, emisiones de voz, transmisión de mensajes, datos o antecedentes, todo lo que va en el impulso eléctrico, dentro de la utilización de una frecuencia".

72 Segundo Informe, Comisión de Transportes y Telecomunicaciones de la Cámara de Diputados, de 18 de enero de 1993, Boletín 400-15, s/n° de pág.

73 Ya Maturana Miquel, Cristián (2002). "Responsabilidad de los proveedores de acceso y de contenido en internet". *Revista Chilena de Derecho Informático*, número 1, pp. 17-30, 22.

74 Álvarez Valenzuela (2005) 201-202; Matus/Ramírez (2014) 301.

75 Matus/Ramírez (2014) 299.

76 Matus/Ramírez (2014) 229, aprecian en el envío de correos electrónicos "una razonable expectativa de privacidad", haciendo referencia además a la doctrina del Tribunal Constitucional (v. nota siguiente).

77 En efecto, en TC. Rol N° 2379-13-INA, el Tribunal Constitucional ha afirmado la protección constitucional de la privacidad de los correos electrónicos, en los que su emisor "singulariza al o a los destinatarios de su comunicación con el evidente propósito de que solo él o ellos la reciban […] [de modo que] los correos electrónicos se enmarcan perfectamente dentro de la expresión "comunicaciones y documentos privados" que utiliza el artículo 19 N° 5° de la Constitución. Estos son comunicaciones, que se transmiten por canales cerrados, no por canales abiertos, y tienen emisores y destinatarios acotados. Por lo mismo, hay una expectativa razonable de que están a cubierto de injerencias y del conocimiento de terceros".

cual la comunicación tiene lugar, cuya percepción por terceros no autorizados exigiría emplear una herramienta o proceso técnico para captar o interceptar la señal en que se transporta y, en su caso, grabarla, que son justamente las hipótesis tipificadas por artículo 36 B, letra c), de la Ley de Telecomunicaciones.

Ahora bien, por lo que respecta a las conductas específicamente sancionadas, la letra c) castiga al que "intercepte" o "capte", en ambos casos de forma maliciosa, o al que sin autorización "grabe" las respectivas señales de telecomunicación. La noción de "interceptar", sugiere una interrupción de la comunicación, esto es, una obstrucción de la vía de comunicación, impidiendo que la señal llegue al destinatario, mientras que la de "captar" se conforma con "percibir", "recibir" o "recoger" esas señales, sin impedir que lleguen a aquel[78].

Si se atiende a la forma como opera la transmisión de correos electrónicos, su captación es posible desde el instante inmediatamente posterior a aquel en que su redactor dio exitosamente a su computador la instrucción de envío, y hasta que el destinatario da al suyo, también exitosamente, la instrucción de "bajar" el mensaje desde el servidor, de modo que se aloja en su computador. Aplicado ello al caso de la intromisión por parte del empleador en los correos electrónicos del trabajador, la conducta podrá realizarse accediendo al servidor de la empresa para captar un mensaje "enviado", antes de que haya llegado a destino, o a un mensaje "recibido" antes de que se descargue en el computador usado por el trabajador o en un dispositivo móvil que le permitiera recibirlo, pues hasta ese momento la comunicación aun está en curso. En estos casos, la conducta del empleador realiza las exigencias objetivas del tipo penal del artículo 36 B, letra c), de la Ley de Telecomunicaciones.

Por lo que respecta a la exigencia típica de "malicia", mayoritariamente se la entiende como una referencia a dolo directo[79], una especie de dolo que, en cualquier caso, también se ve satisfecho con "un dolo de las consecuencias seguras"[80].

---

78 La Comisión de Constitución del Senado añadió, de hecho, el verbo "captar" para dejar en claro, por si alguna duda cupiese, que esta segunda hipótesis también es punible –la percepción, sin impedir que la señal llegue al destinatario–; véase Primer Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, de 30 de marzo de 1993, s/n° de pág.

79 Aunque parte de la doctrina ha puesto en duda que la expresión "malicia" excluya el dolo eventual, aquí se asume como dominante la interpretación que precisamente lo excluye cuando la ley emplea tal expresión; véase, crítico respecto de esta restricción, Hernández, Héctor (2011a). "Artículo 1°". En Couso, Jaime / Hernández, Héctor. *Código Penal Comentado, Parte General*. Santiago: Abeledo Perrot - LegalPublishing, pp. 7-105, 74-75.

80 Véase Hernández, Héctor (2011a) 70.

Por último, en relación con la difusión de la información, de la letra d), basta la difusión privada y, de acuerdo con el tenor literal de la disposición, la conducta se castiga respecto de cualquiera que divulgue el mensaje, sin necesidad de que se trate de la misma persona que lo captó[81].

Una variante de interés puede producirse en el acceso por parte del empleador a los correos electrónicos de una cuenta a la que el trabajador ya no puede tener acceso, tras su desvinculación (por renuncia o despido), con el propósito de obtener información útil para defender los intereses de la empresa, incluso en una eventual demanda en tribunales.

En tal caso, los correos recibidos en esa cuenta, desde el instante de la desvinculación, quedarán alojados en el servidor, sin poder ser "bajados" por el trabajador a un dispositivo al que él tenga acceso. Nuevamente se trataría, entonces, de la captación de comunicaciones en curso, efectuadas mediante señales emitidas a través de un servicio público de telecomunicaciones. El hecho de que esa comunicación probablemente no iba llegar a destino no cambia en nada la base fáctica relevante para el enjuiciamiento. Si se trata de una comunicación privada, enviada por una persona natural a otra persona natural determinada, esta es la única autorizada para percibir su contenido. En este caso, la legítima expectativa del ex trabajador destinatario del mensaje no consiste en que se le dé acceso a esos mensajes, sino en que su cuenta sea dada de baja, de modo que quienes le envíen correos a ella reciban un mensaje automático del servidor, que les permita insistir por otra vía. En cualquier caso, todo ello sería irrelevante. Lo que importa para establecer la tipicidad bajo la modalidad típica de "captación" de señales, como ya se vio, no es la interrupción de la comunicación, sino la percepción o recepción no autorizada de ella, que en esta variante también se produciría. Si acaso la protección de intereses de la empresa justifica esta intromisión es algo que se examinará más abajo[82].

(3.3.3.) Acceso no autorizado y revelación de datos contenidos en sistemas de tratamiento de información, de los artículos 2° y 4° de la Ley de Delitos Informáticos

El artículo 2° de la Ley de Delitos Informáticos 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".*

81 Las razones son idénticas a las que llevan a la Corte Suprema a esa conclusión en relación con el artículo 4° de la Ley de Delitos Informáticos; véase *infra*, 3.3.3.

82 *Infra*, 4.

El artículo 4° de la misma ley, por su parte, castiga al que:

> *"maliciosamente revele o difunda los datos contenidos en un sistema de información".*

Ya 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, tal como ocurría en otros países que habían legislado en la misma dirección[83].

Así lo entiende la doctrina, que precisamente ha destacado la relativa simetría existente entre la protección brindada por estos delitos a la privacidad de los datos informáticos, con la que el artículo 146 del CP ofrece a la privacidad de los "papeles"[84].

La ley, entonces, no solo castiga el *hacking* "duro" o *cracking* del sistema informático o de los datos, destinada a dañar uno u otros, sino también el *hacking* "blando", consistente en el acceso indebido, sin intención de dañar el sistema o los datos[85]. Precisamente eso basta para afectar la privacidad de los datos.

Y, a diferencia de lo que ocurre en otros ordenamientos, como el alemán[86], la violación de la confidencialidad o privacidad de los datos, por intromisión, no requiere que estos se encuentren especialmente asegurados contra el acceso[87], como lo ha reconocido ya alguna jurisprudencia[88].

También es relevante señalar que la jurisprudencia de la Corte Suprema ha reconocido la protección de la privacidad de los datos con independencia de la propiedad sobre el computador en que se encuentra, a

---

83 En la Exposición de Motivos se aprecia el objetivo de poner nuestra legislación a la par de otras, también tenidas en cuenta en este artículo, como la de Alemania y Austria; véase "Historia de la Ley N° 19.223". Disponible en https://www.leychile.cl/Navegar?idNorma=30590&buscar=Historia+de+la+Ley+N%C2%B0+19.223 [fecha de visita: 30 de noviembre de 2015], p. 5. En particular, la protección de la privacidad y de la intimidad, a través de uno de los tipos penales que finalmente se incorporan a la ley, es destacada por el entonces Ministro de Justicia, Francisco Cumplido (p. 30) y por la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, en su Segundo Informe, de 18 de agosto de 1992 (p. 34).

84 Véase *supra*, 3.2.2. También se hace referencia a la "confidencialidad" de los datos para designar el bien jurídico protegido; véase Moscoso (2010) 30.

85 Moscoso (2010) 33.

86 Véase *supra*, 3.3.1.

87 Moscoso (2010) 38.

88 Sentencia del Cuarto Tribunal de Juicio Oral en lo Penal de Santiago. 2 de septiembre de 2009. RIT 135-2009, RUC 0700879841-3, considerando tercero, citado por Moscoso (2010) 38, nota al pie 41.

favor de los datos que un funcionario guarda en el computador que le ha sido facilitado para desempeñar sus funciones[89].

Por lo que respecta al artículo 4°, la difusión no tiene por qué ser hecha a un gran número de personas. Según la misma Corte Suprema, hubo difusión en la conducta consistente en dar conocimiento de la información a la que se accedió indebidamente a otras tres personas[90]. En el derecho alemán, sobre una base normativa semejante a la chilena, se acepta que hay difusión incluso en el acto de entregar la información a las autoridades de persecución penal, sin perjuicio de que pueda luego discutirse si esa conducta –indudablemente típica– se encuentra justificada[91].

Por último, la Corte Suprema también afirma, como por lo demás viene sugerido por el tenor literal, que, para ser sancionado, no es necesario que quien revela los datos haya sido la misma persona que accedió ilícitamente a ellos[92].

El tenor de estas disposiciones no parece oponer problemas, *prima facie*, para subsumir en ellas la intromisión del empleador en los correos electrónicos del trabajador. Pues en tal caso se accede a datos de un sistema de tratamiento de los mismos, el servidor del remitente del correo electrónico, sin autorización de alguno de los titulares de los datos –el remitente o el destinatario–.

Ahora bien, la circunstancia de que el acceso por parte del empleador se produzca en terminales y servidores de su propiedad plantea la siguiente cuestión: ¿Qué relación debe tener el titular de los datos con el sistema de tratamiento de los mismos al cual el tercero accedió indebidamente? Es claro que no tiene por qué tener propiedad sobre ellos. Pero, ¿debe tener la facultad de acceder a él o de autorizar a otro que acceda al mismo? La disposición nada dice, pero la analogía con el caso del computador puesto a disposición del trabajador o funcionario, respecto del cual este tiene ciertamente una facultad de acceso y en su caso, de permitir a otro hacerlo, sugiere que el titular de los datos no puede ser ajeno al computador o sistema de tratamiento de datos. La finalidad de protección del tipo sugiere, de hecho, que el sistema de tratamiento de datos debe ser uno sobre el cual el titular de los datos puede ejercer el poder de acceder, y de permitir o negar el acceso a otros, sin que esto último suponga, como se

89 Corte Suprema. 20 de marzo de 2013. Rol N° 3951-2012. "C/ Sergio Valenzuela Cruz y otros". No disponible en colecciones físicas o electrónicas.

90 CS. Rol 3951-2012.

91 Schuster, Frank Peter (2010). "IT-gestützte interne Ermittlungen in Unternehmen – Strafbarkeitsrisiken nach den §§ 202a, 206 StGB". *Zeitschrift für Internationale Strafrechtsdogmatik*, 2010, vol. 12/2015, pp. 68-75, p. 72.

92 CS. Rol 3951-2012.

vio, medida de seguridad alguna, pero sí al menos, la posibilidad de permitir un acceso lícito.

¿Se encuentra en esa situación el servidor del correo electrónico del destinatario de este? Bien vista su situación, me parece que sí. El titular de la cuenta de correo electrónico tiene la facultad de acceder a la información que, bajo su nombre de usuario, y mediante uso de su clave secreta, se encuentra alojada en el servidor. Él puede permitir a otros el acceso y, ciertamente, puede negarles el acceso.

Nada hay, pues, en el tenor literal de la disposición, que se oponga a subsumir en el tipo la intromisión del empleador, siempre que se satisfaga, además, la exigencia subjetiva de que el acceso haya sido efectuado con el ánimo de conocer indebidamente la información.

Sin embargo, dado que la intromisión del empleador en los correos electrónicos del trabajador lo más probable es que se produzca mientras el correo electrónico aun está alojado en el servidor, al que el empleador (en general, a través de su departamento de informática) suele tener acceso directo, esa conducta no solo realizaría el tipo de acceso indebido a la información, del artículo 2° de la Ley de Delitos Informáticos, sino también la del artículo 36 B, letra c), de la Ley de Telecomunicaciones, pues se trataría de una comunicación que está aun siendo transmitida, y se encuentra protegida contra la captación no autorizada[93]. En mi opinión, en tal hipótesis nos encontraríamos ante un concurso aparente de leyes penales, que debe resolverse por subsidiariedad (tácita) a favor del tipo penal de interceptación o captación de señales de telecomunicaciones, sancionado con una pena ligeramente superior a la de acceso indebido a un sistema de tratamiento de información, que expresa un interés del legislador también (ligeramente) superior en la protección –junto con la privacidad de la comunicación– de la inviolabilidad de los servicios públicos de telecomunicaciones, en comparación con su interés en proteger la inviolabilidad de los sistemas informáticos. En cambio, si la intromisión del trabajador se produce cuando la comunicación ya no puede entenderse aun en transmisión, por ejemplo, cuando el correo ya fue "bajado" y alojado en su computador, la conducta debe sancionarse como acceso no autorizado a datos informáticos, con el ánimo de conocerlos.

93 Véase *supra*, 3.3.1.

(3.4.) Falta de autorización o de voluntad por parte del titular de los datos o comunicaciones

Como se señaló más arriba, a los tres tipos que se ven realizados, siquiera en una primera consideración, por la intromisión del empleador en los correos electrónicos del trabajador, es común la exigencia de que el agente no cuente con la autorización del titular de la información privada a la que accede. Se trata de un elemento normativo del tipo, de carácter jurídico, formulado de manera negativa: el agente no debe haber contado con la debida autorización. Tal exigencia es explícita en el artículo 146 del CP y en el artículo 36 B, letra c), de la Ley de Telecomunicaciones, y debe entenderse como exigencia implícita del artículo 2° de la Ley de Delitos Informáticos, en relación con la cualidad de "indebido" del conocimiento buscado por el agente.

Es trivial que la "debida autorización" en el artículo 36 B, letra c), de la Ley de Telecomunicaciones puede ciertamente referirse a la de la autoridad judicial[94]. Más interesante es examinar las condiciones bajo las cuales puede tenerse por concurrente una autorización del titular de la información o comunicación en el caso relativamente habitual, en la práctica empresarial, de que el reglamento interno de la empresa califique la casilla de correo electrónico proporcionada a sus trabajadores como una "herramienta de trabajo", y se reserve el derecho de acceder a su contenido, reglamento interno que a los trabajadores, con frecuencia, se solicita firmar en señal de consentimiento. Estas cláusulas suelen tener el sentido de permitir a los encargados informáticos proteger la integridad de los sistemas informáticos y la confidencialidad de los datos de la empresa y de la correspondencia oficial.

¿Es suficiente esa circunstancia para considerar que el titular de la información y de la comunicación autoriza a la empresa a captar y abrir su correspondencia electrónica privada y a acceder a y registrar los documentos electrónicos asociados a tales comunicaciones, para enterarse de su contenido?

Las mejores razones llevan a concluir que no. El titular de la información no da tal autorización.

---

94 Autorización regulada por los artículos 218 y 222 del Código Procesal Penal y por el Reglamento sobre Interceptación y Grabación de Comunicaciones Telefónicas y de otras formas de Telecomunicación, dictado mediante el Decreto N° 142 del Ministerio de Transporte y Telecomunicaciones (Diario Oficial 22/9/2005). Si bien, a primera vista, pareciera que el artículo 218 del CPP cubre todas las hipótesis de incautación de correspondencia electrónica imaginables, la que aún se encuentra siendo transmitida (véase *supra*, 3.3.2.) solo es accesible interceptando una señal de telecomunicación, una hipótesis regulada por el artículo 222, inc. 1°, *in fine*, del CPP.

Como se observó más arriba[95], de acuerdo con la doctrina de la Dirección del Trabajo y del Tribunal Constitucional, las comunicaciones privadas, aun sostenidas por medio de una casilla de correo electrónica habilitada por el empleador, se encuentran protegidas por la garantía constitucional de la inviolabilidad de correspondencia y de las comunicaciones privadas. Esta protección no desaparece porque la empresa se arrogue una potestad unilateral de revisar los correos electrónicos. Y tampoco es renunciable por un trabajador, tratándose de una garantía constitucional, como ha dictaminado la Dirección del Trabajo[96].

Ello no quiere decir, sin embargo, que un trabajador no pueda renunciar al carácter privado de una comunicación, precisamente autorizando a terceros a acceder a su contenido. Ya no se trataría, entonces, de una renuncia a la garantía constitucional de la inviolabilidad de las comunicaciones privadas, sino de una autorización expresa del trabajador de que se acceda al contenido de una comunicación privada. Así, por ejemplo, si un trabajador enfermo en casa, telefónicamente autoriza a un compañero de trabajo o a su jefe para abrir su correo electrónico para que así estos puedan revisar si ha recibido alguna comunicación que estaba esperando y a la cual es importante responder con urgencia, no está renunciando a la protección que la garantía constitucional de la inviolabilidad de las comunicaciones privadas le brinda, sino al carácter privado de una comunicación en particular.

¿Y no es posible deducir del carácter oficial de la cuenta de correo electrónico una autorización general del trabajador al empleador para consultar sus mensajes?

En Chile el tema no se ha planteado en sede penal, pero el Tribunal Constitucional ha sugerido, respecto de los correos electrónicos enviados y recibidos por funcionarios públicos, a través de sus casillas institucionales, que se asume su carácter privado, a no ser que esté expresamente prohibido el uso privado de tales casillas[97].

---

95 *Supra*, 2.

96 "[E]l empleador podrá regular las condiciones del uso de los correos electrónicos […] pero en ningún caso –ni por reglamento interno ni por acuerdo de las partes– podrá regularse el ejercicio mismo de la respectiva garantía constitucional […] [Y esto] no podría ser de otra forma, si se tiene presente que aún las regulaciones legales de una garantía constitucional autorizadas por la propia Constitución "*no podrán afectar los derechos en se esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio*" […]", Dictamen de la Dirección del Trabajo Ord. Nº 260/019 de 24 de enero de 2002 (la cursiva está en el original).

97 Tribunal Constitucional. 29 de enero de 2014. Rol N° 2379-13-INA, considerando trigésimo, afirmando que a falta de tal prohibición expresa, se permite el uso privado, en el contexto de una sentencia que, además, como se vio, *supra* 3.2, reconoció el carácter privado de los correos electrónicos enviados y recibidos en esas casillas institucionales.

En ese contexto, de la firma del reglamento interno en el que la empresa se reserva el derecho a acceder al contenido de los correos de las cuentas asignadas a los trabajadores difícilmente puede afirmarse que el trabajador autoriza el registro de todas sus comunicaciones privadas, mantenidas a través de la cuenta de correo electrónico unipersonal que le proporcionó la empresa, identificada justamente con su nombre. El reglamento interno, cualquiera que fueren sus términos, no podría imponer a los trabajadores, incluso si se les exigió firmar un recibo, la renuncia a la garantía de la inviolabilidad de la correspondencia. Eventualmente podría haber prohibido el uso privado de los mismos, pero tampoco puede desprenderse de ello, sin más, que los trabajadores renunciaban a la privacidad de las comunicaciones efectuadas por ese medio[98].

Así, respecto del trabajador que firma el reglamento interno, a lo más puede afirmarse que es consciente de que su cuenta de correo electrónico puede ser monitoreada por la empresa, con un fin muy específico: asegurar la integridad de los sistemas informáticos de la empresa y garantizar la reserva y confidencialidad de las operaciones de carácter profesional que a través del correo electrónico efectúa, es decir, para garantizar que terceros ajenos a la empresa no tengan acceso a tales operaciones, que es la única confidencialidad que a la empresa puede interesarle. Pero no cabe desprender de ello que ese trabajador accede a que incluso sus comunicaciones extralaborales sean registradas. Eso nada tiene que ver con la integridad de los sistemas informáticos y la garantía de la reserva y confidencialidad de operaciones de carácter profesional. El trabajador que declara conocer el Reglamento puede seguir confiando, entonces, en que sus comunicaciones privadas no serán registradas.

Por lo demás, la clara doctrina de la Dirección del Trabajo, conforme a la cual, ni aun con acuerdo del trabajador, la regulación en el uso de los correos electrónicos por parte de la empresa, puede traducirse en que ella conozca el contenido de los mismos, puede entenderse como un argumento en contra de la eficacia de una supuesta renuncia anticipada, *in totum*, a la privacidad de los correos electrónicos enviados y recibidos desde cuentas unipersonales. Tal renuncia debería efectuarse de forma singular, en términos acotados.

98 Ténganse en cuenta, al efecto, los categóricos términos con que el Dirección del Trabajo afirma el carácter privado de toda comunicación recibida en las cuentas unipersonales del trabajador, aun si la empresa ha prescrito que todo mensaje enviado desde ellas debe ir con copia a la gerencia. De ello parece desprenderse que, si el trabajador infringió esa prohibición, podrá haber consecuencias laborales, pero no cabe presumir que el trabajador haya autorizado la revisión de las comunicaciones que sostuvo (aun en contra de la prohibición).

Sin embargo, otra cosa cabe concluir si el carácter colectivo o compartido de la cuenta descarta la existencia de una expectativa de privacidad de las comunicaciones. La cuestión se ha planteado en el derecho alemán, donde la doctrina ha entendido que falta el carácter privado en el mensaje electrónico cuando está dirigido a una cuenta colectiva de la empresa (por ejemplo: adquisiciones@empresaimaginaria.cl), afirmando, por el contrario, el carácter privado de todo mensaje dirigido a una cuenta unipersonal, a nombre del trabajador (por ejemplo, pedro.perez@empresaimaginaria.cl)[99]. En el primer caso habría que incluir también a las cuentas que, con conocimiento del trabajador, emiten automáticamente una copia de todo mensaje enviado o recibido a través de ellas a un oficial o departamento de *compliance*.

4) Posible concurrencia de una causal de justificación

No es posible en este lugar, ni es el objetivo de este trabajo, analizar exhaustivamente las causas de justificación que podrían venir al caso respecto de una intromisión en los correos electrónicos de los trabajadores. Pero hay un par de situaciones paradigmáticas que merecen siquiera una breve mención, sobre todo para dar cuenta de dónde parece tener sentido efectuar una indagación específica respecto de la posible concurrencia de causas de justificación.

La intromisión por parte del empleador puede estar presidida, en primer lugar, por su interés en precaver un perjuicio patrimonial a la empresa frente a atentados del trabajador, sea contra sus activos físicos o financieros, por ejemplo a través de delitos de apropiación, sea contra la propiedad industrial de la empresa, por ejemplo a través de la divulgación de secretos industriales o empresariales. En segundo lugar, el empleador puede tener un interés en hacer efectiva la responsabilidad del trabajador o ex trabajador –en sede penal o civil– por un perjuicio ya irrogado o, simplemente, un interés en probar –en sede laboral– un incumplimiento grave del contrato de trabajo por parte del trabajador, u otra causal de despido de las que no dan derecho al trabajador a indemnización.

[99] Eisele (2012) 405.

Interés en precaver perjuicios para la empresa

Para esta primera hipótesis, cabe preguntarse, en primer lugar, si podría venir al caso la justificante de legítima defensa[100].

Esta justificante requiere, en primer lugar, de conformidad con el artículo 10, números 4º, 5º y 6º, del CP la presencia de una "agresión ilegítima", actual o inminente[101]. Los delitos ya perpetrados, en este caso, no cuentan, pues constituyen una agresión ya agotada frente a la cual no cabe "defensa" sino solo una posible reacción punitiva (cuya justificación habría que buscar, si cabe, en otra causal, como se verá más abajo). Con todo, la existencia de indicios claros de actividad delictual previa de un trabajador contra la empresa puede fundamentar, teniendo en cuenta las circunstancias del caso, un peligro inminente de reiteración, que podría constituir una nueva agresión de la cual el empleador podría estar en situación de tener que defenderse. Una dificultad ante la cual seguramente se encontrará el empleador es que, para tener por configurada la realidad de la agresión –requisito indispensable para que la intromisión esté justificada como "defensa"– precisamente le faltará la información de la que pretendía hacerse revisando los correos del trabajador. Es decir, en vez de certezas sobre el hecho de que el trabajador está atentando contra los intereses patrimoniales de la empresa, con frecuencia tendrá, a lo sumo, sospechas más o menos fundadas. Pero las sospechas no bastan, si finalmente resulta que la agresión no era real (según un juicio objetivo *ex post*), o si al momento de la intromisión ella no era ostensible (según un juicio objetivo *ex ante*). Ahora bien, si el empleador, a partir de indicios serios de que se está produciendo un atentado a sus intereses patrimoniales, se convence de que la agresión es real, y luego resulta que la revisión de los correos no confirma la efectividad de la agresión, ¿no se configuraría entonces una legítima defensa putativa? Efectivamente, podría darse esa constelación y, de ser así, el error del empleador, aun vencible, juega a su favor en la medida que, según la doctrina dominante, esa especie de error (en los presupuestos fácticos de la justificante) excluye la posibilidad de sancionar

100 El análisis dogmático que se ofrece a continuación no se apoya en precedentes doctrinarios y jurisprudenciales, pues la cuestión apena si se ha planteado. En el derecho comparado, la invocación de una legítima defensa o de un estado de necesidad justificante solo parece tener cabida para justificar conductas de interceptación que consistan en impedir que la comunicación llegue a destino. Ahí pueden tener sentido, por ejemplo, la legítima defensa o el estado de necesidad, para proteger el sistema informático del empleador en contra de un mensaje con virus o "troyanos"; véase Eisele (2012) 406.

101 Sobre los requisitos de la legítima defensa y para todas las referencias que en este lugar se hará a ellos véase, por todos, sintéticamente, Couso, Jaime (2011a). "Artículo 10, nº 4º". En Couso, Jaime / Hernández, Héctor. *Código Penal Comentado, Parte General*. Santiago: Abeledo Perrot - LegalPublishing, pp. 209-226.

su conducta a título de dolo, dejando solo subsistente la culpa solo para el evento de que la conducta respectiva esté también tipificada como cuasidelito, algo que no ocurre con los tipos aplicables a la intromisión en los correos electrónicos ajenos. Esto jugará a favor del empleador de buena fe. Sin embargo, la defensa putativa solo será plausible si la apariencia de agresión fuere, desde la perspectiva del empleador, realmente convicente. Nuevamente, las meras sospechas no bastan[102].

En seguida, el medio escogido por el empleador para impedir o repeler esa agresión –captar y, en su caso, difundir los correos electrónicos del trabajador– debe ser idóneo para lograrlo. La satisfacción de este requisito seguramente dependerá del tipo de activos objeto de agresión y de defensa: si se trata de atentados a los activos físicos de la empresa (como en el hurto de especies que se encuentran más o menos a disposición del trabajador) es dudoso que la intromisión en los correos electrónicos del trabajador que está cometiendo la conducta sea un medio idóneo para impedirlo; en cambio, dado su carácter inmaterial, tal intromisión sí podría llegar a ser idónea para identificar el modo de los ataques –y así poder interrumpirlos– contra activos financieros o contra la propiedad intelectual o industrial de la empresa. Pero, nuevamente, no bastaría con que a través de ese medio solamente se pretenda fundar una acción judicial contra el trabajador o ex trabajador dirigida a sancionar el perjuicio ya producido. Sería necesario que efectivamente la interceptación de correos electrónicos sea, siquiera desde una perspectiva objetiva *ex ante*, idónea para impedir (o "repeler", si cabe) nuevos ataques inminentes al patrimonio de la empresa. Las circunstancias del caso –entre ellas, que se trate de un trabajador aun en funciones, y no ya despedido– podrían efectivamente justificar ese pronóstico (si además consta la inminencia de una muy probable reiteración).

Por lo que respecta a la exigencia de necesidad racional del medio empleado para impedir o repeler la agresión, solo se verá satisfecha si otras medidas de protección más directa a los activos de la empresa no son practicables. Pero el caso es que, en la gran mayoría de los casos, el alejamiento del trabajador –de cuya participación en la agresión ya se cuenta con evidencias objetivas (de lo contrario, no se verá satisfecha la

[102] Irónicamente, sin embargo, si pese a la falta de todo indicio serio de que el atentado se estaba produciendo, tras la intromisión (efectuada por una pura corazonada del empleador) se comprueba que ello efectivamente era así, según la doctrina dominante en Chile, que prescinde de la exigencia de elementos subjetivos en la legítima defensa, la existencia objetiva (desde la perspectiva *ex post*) de la agresión bastaría, sin que sea necesario que el que se defiende haya tenido noticias ciertas sobre ello. Sin embargo, como se señala en el texto principal, todavía sería necesario satisfacer los restantes requisitos de la justificante, algo no muy fácil de lograr.

exigencia de "realidad" de la agresión)– bastará para impedir la reiteración; añadir a eso la violación de su correspondencia representaría un "exceso intensivo" en la legítima defensa.

Por último, la exigencia de que la empresa o el empleador no hayan provocado la agresión del trabajador no presenta particularidades en las hipótesis examinadas, y será raro que no se vea satisfecha (pero casi tan raro como ello será que se hayan satisfecho los demás requisitos, como para que llegue a ser necesario examinar este).

En relación con el estado de necesidad justificante[103], no siendo aplicable el contemplado por el artículo 10, nº 7º, del CP, que por disposición expresa de la ley solo permite justificar daños irrogados en la "propiedad ajena" (y no, en cambio, uno irrogado a la inviolabilidad de las comunicaciones), si se le entiende también incluido –y con un alcance más amplio que el del numeral 7º– como causal de justificación, en el numeral 11 del artículo 10 del CP[104], solo sería aplicable frente a perjuicios que puedan ser calificados jurídico-penalmente de un "mal" y, al igual que en la legítima defensa, siempre que la intromisión sea idónea para evitarlo. Entonces, otra vez, el interés en obtener información sobre el responsable de un mal ya acaecido, con la cual poder apoyar la iniciación de acciones penales o civiles o de constituir una causal de término del contrato de trabajo, no va en línea con esa exigencia de idoneidad para la evitación del mal, a menos que se identifique como mal la "impunidad" o la imposibilidad de hacer efectiva la responsabilidad civil o de terminar el contrato de trabajo sin indeminización. Pero conceptualizado el mal así, muy dificilmente se cumplirán los restantes requisitos del estado de necesidad: la proporcionalidad (que el mal causado –la lesión a la inviolabilidad de las comunicaciones– sea menor que el que se evita) y la subsidiariedad (que no haya otro medio practicable y menos perjudicial para evitar el mal).

En cambio, frente a un perjuicio para el patrimonio de la empresa cuyo acaecimiento aún sea actual o inminente habría menos dificultades

103 Sobre las exigencias del estado de necesidad y, nuevamente, para todas las referencias que en este lugar se hará a ellos véase, por todos, sintéticamente, Hernández, Héctor (2011b). "Artículo 10, nº 11". En Couso, Jaime / Hernández, Héctor. *Código Penal Comentado, Parte General*. Santiago: Abeledo Perrot - LegalPublishing, pp. 266-275

104 Así, Cury, Enrique (2013). "El estado de necesidad en el Código Penal Chileno". En AA.VV. *La ciencia penal en la Universidad de Chile. Libro Homenaje a los Profesores del Departamento de Ciencias Penales de la Facultad de Derecho de la Universidad de Chile*. Santiago: Facultad de Derecho de la Universidad de Chile, pp. 249-267, 252 y ss. véase, con todo, a favor de interpretar ese precepto únicamente como causal de exculpación, Hernández, Héctor (2011b). "Artículo 10, nº 11". En Couso, Jaime / Hernández, Héctor. *Código Penal Comentado, Parte General*. Santiago: Abeledo Perrot - LegalPublishing, pp. 266-275, 270-271.

para afirmar la idoneidad de la intromisión para evitarlo (sobre todo, si se trata de atentados a activos inmateriales). En todo caso, la justificante sería aplicable a casos en que ese riesgo no provenga de una conducta del propio trabajador que pueda considerarse como una "agresión de su parte" (por ejemplo, si se tiene antecedentes de que un tercero está obteniendo del trabajador, mediante engaño, secretos industriales de la empresa). En esta hipótesis, con todo, sigue siendo necesario examinar si acaso se cumplen las exigencias de proporcionalidad y subsidiariedad. La primera exige una ponderación que es difícil de resolver: ¿es más grave exponer las comunicaciones privadas del trabajador, revisando su correspondencia electrónica, que arriesgar, por ejemplo, la divulgación de información valiosa para la empresa? La respuesta depende, probablemente, de varios factores que especifican el peso de cada interés.

Y aun si ese ejercicio de ponderación se resuelve a favor de la revisión del los correos electrónicos del trabajador, todavía es necesario examinar si se cumple el requisito de subsidiariedad: ¿no es posible, instruir al propio trabajador sobre los riesgos?, ¿o pedir su consentimiento para que un solo funcionario, especialista en el análisis de riesgos para los secretos industriales, examine sus correos, con obligación de reserva?, ¿o solicitar autorización judicial de modo que haya un control más estricto sobre la necesidad de la intromisión, y su extensión? Si cualquiera de esas opciones es practicable, este requisito del estado de necesidad justificante no se cumplirá.

Un caso de interés en el derecho comparado se presenta a propósito del interés (patrimonial) de la empresa en optimizar el uso del tiempo por parte de los trabajadores, impidiendo que sus comunicaciones los distraigan en exceso. Pero precisamente aquí es difícil imaginar que la revisión del contenido de sus mensajes sea un medio proporcional y estrictamente necesario *vis-à-vis* otros menos perjudiciales para el trabajador (como el monitoreo del tiempo invertido por el trabajador en –y no del contenido de– su correo electrónico[105]).

Sobre la exigibilidad del sacrificio del bien (del empleador o la empresa) amenazado, no parece haber particularidades, y será raro que llegue

[105] Así lo ha entendido, por ejemplo, el *Working Party on the Protection of Individuals with regard to the Processing of Personal Data*, establecido por la Unión Europea (de conformidad con lo dispuesto en el Art. 29 de la Directiva 95/46/EC), en su informe "Working document on the surveillance of electronic communications in the workplace", p. 17 (disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf, visitada el 21 de abril de 2017): "Proportionality [...] The monitoring of e-mails should, if possible, be limited to traffic data on the participants and time of a communication rather than the contents of communications if this would suffice to allay the employers concerns".

a afirmarse (de nuevo, casi tan raro como ello será que llegue a ser necesario examinar este último requisito).

Interés en hacer efectiva la responsabilidad del trabajador o en despedirlo sin derecho a indemnización

Por lo que concierne a la interceptación o apoderamiento de los correos electrónicos de un trabajador para perseguir su responsabilidad penal o civil, cuando ya atentó contra los intereses de la empresa, o de despedirlo sin derecho a ser indemnizado, como ya se señaló, difícilmente podría justificarse a través de la legítima defensa o del estado de necesidad justificante.

La posibilidad de justificar la intromisión en base a ese interés del empleador se discute, más bien, a propósito de la justificante de ejercicio legítimo del derecho[106], precisamente el derecho del empleador a perseguir la responsabilidad del trabajador. Con todo, dado que las condiciones de aplicación de una medida de estas características se encuentran estrictamente reguladas en el ordenamiento jurídico, en los artículos 218 y 222[107] del CPP y el reglamento sectorial que operacionaliza su implementación de lo dispuesto por el segundo de ellos[108], no parece posible calificar de "ejercicio legítimo" de un derecho a un acto que se salta las formalidades exigidas por esa regulación. Y si bien, en contra de la doctrina que reconoce esta justificante solo cuando la ley expresamente faculta la realización de una conducta típica, otra opinión doctrinaria admite que la autorización puede deducirse de normas consuetudinarias o reconocerse mediante una interpretación analógica[109], ello solo parece tener sentido como un recurso para reconocer un derecho en el silencio de la ley, pero no contra texto expreso de una ley que, como en este caso, establece las condiciones estrictas bajo las cuales procede el acto, previa orden judicial y cumpliendo con las demás formalidades legales y reglamentarias[110].

106 Romeo Casabona, Carlos María (2002). "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de internet". *Derecho y Conocimiento*, vol. 2, pp. 123-149, 147. Disponible en: https://www.unifr.ch/ddp1/derechopenal/obrasportales/op_20080612_17.pdf [fecha de visita: 24 de noviembre de 2015].

107 Véase supra, n. 94.

108 Reglamento sobre Interceptación y Grabación de Comunicaciones Telefónicas y de otras formas de Telecomunicación, dictado mediante el Decreto N° 142 del Ministerio de Transporte y Telecomunicaciones (Diario Oficial 22/9/2005).

109 Véanse los detalles en Couso, Jaime (2011) 263.

110 En el derecho alemán, la autorización para apoderarse de datos contenidos en comunicaciones portadas en medios electromagnéticos también parece reducirse al caso en que se cumplan las formalidades legales establecidas por las diversas leyes que, con finalidad de per-

Ahora bien, si el interés del empleador consiste en ejercer una acción civil o probar en sede laboral que se ha configurado una causal de despido sin indemnización, y no en cambio en perseguir la responsabilidad penal del trabajador ¿queda liberado de las restricciones que han sido establecidas, únicamente para la sede penal? Esa pretensión sería absurda. Pues es del todo contraintuitivo suponer que la protección de la privacidad de las comunicaciones electrónicas frente al interés en la persecución de responsabilidad civil, o frente al interés en poner término al contrato de trabajo, es más baja que frente al interés en perseguir la responsabilidad penal. El hecho de que no estén reguladas las condiciones de una autorización judicial en estas otras sedes difícilmente puede interpretarse en el sentido de que aquí es más sencillo –que en sede penal– invocar el ejercicio legítimo del derecho para justificar una intromisión decidida por el empleador por sí y ante sí; por el contrario, la falta de regulación parece dar cuenta de que el interés en proteger la privacidad de las comunicaciones electrónicas, a lo menos por regla general, no puede ceder ante los intereses probatorios en causas civiles o laborales, de modo que el juez no contaría en esas jurisdicciones con facultades para ordenar la intervención de tales comunicaciones.

Conclusiones

Los correos electrónicos del trabajador gozan de protección constitucional, aun si son enviados o recibidos a través de cuentas de correo habilitadas por el empleador para el ejercicio de las funciones del trabajador, siendo además irrelevante si la intromisión se produce en terminales o servidores de propiedad de la empresa.

La intromisión del empleador en los correos electrónicos del trabajador es una conducta penalmente relevante. Del análisis efectuado, resulta claro, sin embargo, que no lo es bajo la figura del artículo 161-A del CP. Por lo que respecta al artículo 146 del CP, pese a que desde el punto de vista semántico nada obstaría a considerarla derechamente como una hipótesis de "apertura de correspondencia" o "registro de papeles" (en tanto que "documentos"), al haber el legislador creado tipos especiales de interceptación de señales de telecomunicaciones y de acceso al contenido de sistemas de tratamiento de información, restringió el significado de las voces "correspondencia" y "papeles", dejando fuera del alcance del

secución penal o de prevención de ciertos delitos, contemplan tales permisos; véase Kargl (2013) § 202b, nm 8, en relación con el § 202a, nm 17.

artículo 146 del CP las hipótesis de intromisión en los correos electrónicos. Esta interpretación restrictiva, sin embargo, solo está al alcance de quienes entiendan que el correo electrónico efectivamente está protegido por estas otras leyes especiales. Más específicamente, quien considere que el tipo del artículo 36 B de la Ley de Telecomunicaciones no protege al correo electrónico que está siendo transmitido, no tiene razones para excluir este medio de comunicación del alcance del delito de apertura de correspondencia, del artículo 146 del CP. A su vez, quien considere (algo bastante más difícil de imaginar) que los correos alojados en un computador no son datos protegidos por el delito de acceso indebido a un sistema de tratamiento de información, del artículo 2° de la Ley de Delitos Informáticos, tampoco contaría con razones contra su protección a través de la figura de registro de papeles, del mismo artículo 146 del CP.

Ahora bien, si se admite (como se sostiene en este trabajo) que los tipos de la Ley de Telecomunicaciones y de la Ley de Delitos Informáticos son aplicables a los correos electrónicos, la aplicación de uno u otro depende de si los correos aún constituyen una comunicación en curso o si ya se encuentran alojados en un computador. A la primera hipótesis se aplica únicamente la figura de captación de señales de telecomunicaciones, desplazándose (por subsidiariedad tácita) la de acceso no autorizado a datos de un sistema informático, figura esta que justamente solo se aplica a la segunda hipótesis mencionada.

La autorización genérica proporcionada por un trabajador a la empresa, como la que suele exigírsele al suscribir los reglamentos internos, para que la empresa pueda acceder al contenido de sus correos, no constituye una renuncia válida a la inviolabilidad de sus correos electrónicos privados y no vuelve atípica ni justifica la conducta de intromisión, a efectos penales. Pero el uso de cuentas compartidas o colectivas de carácter claramente institucional, o de aquellas que, con conocimiento del trabajador, emiten automáticamente una copia al oficial de *compliance*, dan cuenta de la inexistencia de una expectativa de privacidad.

Por último, aun sin autorización válida del trabajador, la intromisión podría, en casos excepcionales, estar justificada. La legítima defensa podría tener lugar, teóricamente, cuando el empleador de ese modo defiende intereses patrimoniales de la empresa frente a una agresión real del trabajador, que aún está en curso y cuya inminente reiteración podría agravar el daño. Sin embargo, en primer lugar, la mera sospecha del empleador de que ese atentado está teniendo lugar no constituye una agresión real que pueda justificar la intromisión, ni aun configurar una defensa putativa, y, en segundo lugar, los restantes requisitos de la legítima defensa –en espe-

cial, la necesidad racional del medio– rara vez se verán satisfechos. Por lo que atañe al estado de necesidad justificante, sus requisitos difícilmente se verán satisfechos ante una intromisión del empleador dirigida a evitar males no constitutivos de agresiones por parte del trabajador titular de las comunicaciones intervenidas. Por último, tratándose del interés del empleador en ejercer acciones en contra del trabajador ante los tribunales, sin autorización judicial –únicamente disponible, por lo demás, en sede penal– tal interés no bastará para configurar la justificante de ejercicio legítimo del derecho.

Bibliografía citada

Álvarez Valenzuela, Daniel (2005). "Inviolabilidad de las comunicaciones electrónicas". *Revista Chilena de Derecho Informático*, Nº 5, pp. 191-202.

Bascuñán Rodríguez, Antonio (2005). "Delitos contra los intereses personalísimos". *Revista de Derecho de la Universidad Adolfo Ibáñez*, Número 2, pp. 531-556.

Bascuñán Rodríguez, Antonio, (2014). "Grabaciones subrepticias en el Derecho penal chileno. Comentario a la sentencia de la Corte Suprema en el caso Chilevisión II". *Revista de Ciencias Penales*, Sexta época, Vol. XLI, N° 3, pp. 43-74.

Couso, Jaime (2011a). "Artículo 10, n° 4°". En Couso, Jaime / Hernández, Héctor. *Código Penal Comentado, Parte General*. Santiago: Abeledo Perrot - LegalPublishing, pp. 209-226.

Couso, Jaime (2011b). "Comentario a previo los Arts. 74 y 75. En Couso, Jaime / Hernández, Héctor. *Código Penal Comentado, Parte General*. Santiago: Abeledo Perrot - LegalPublishing, pp. 625-666.

Cury, Enrique (2013). "El estado de necesidad en el Código Penal Chileno". En AA.VV. *La ciencia penal en la Universidad de Chile. Libro Homenaje a los Profesores del Departamento de Ciencias Penales de la Facultad de Derecho de la Universidad de Chile*. Santiago: Facultad de Derecho de la Universidad de Chile, pp. 249-266.

Díaz Tolosa, Regina (2007). "Delitos que vulneran la Intimidad de las Personas: Análisis crítico del artículo 161-A del Código Penal Chileno", *Ius et Praxis*, versión On-line, véase 13 n° 1, s/n° de pág. Disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122007000100011 [fecha de visita: 21 de noviembre de 2015]

Eisele, Jörg (2012). "Arbeitnehmerüberwachung und Compliance unter Berücksichtigung der Cybercrime-Konvention". *Zeitschrift für Internationale Strafrechtsdogmatik*, 2010, vol. 8-9/2012, pp. 402-408.

Etcheberry, Alfredo (1998) *Derecho Penal. Parte Especial.* 3ª edición revisada y actualizada. Santiago: Editorial Jurídica de Chile. Tomo III.

Garrido, Mario (2010) *Derecho Penal, Parte Especial*. 4ª edición. Santiago: Editorial Jurídica de Chile. Tomo III.

Hernández, Héctor (2011a). "Artículo 1°". En Couso, Jaime / Hernández, Héctor. *Código Penal Comentado, Parte General*. Santiago: Abeledo Perrot – LegalPublishing, pp. 7-105.

Hernández, Héctor (2011b). "Artículo 10, n° 11". En Couso, Jaime / Hernández, Héctor. *Código Penal Comentado, Parte General*. Santiago: Abeledo Perrot – LegalPublishing, pp. 266-275.

Hoeren, Thomas (2001). "Briefgeheimnis im Strafrecht und E-Mail in Ö und D, Ein Microvergleich". En *Universitätslehrgang für Informationsrecht und Rechtsinformation – Rechtswissenschaftliche Fakultät Wien.* Viena: Max W. Mosin.

Kargl (2013). "§ 202 StGB". En Kindhäuser, Urs / Neumann, Ulfried / Paeffgen, Hans-Ulrich (Editores), *NomosKommentar, Strafgesetzbuch*. 4ª edición. Baden-Baden: Nomos. Vol. II, § 202, nm 3 y ss.

Lewisch, Peter (2008). "§ 118 StGB". *Wiener Kommentar zum Strafgesetzbuch*. 2ª edición. Viena: Manz Verlag.

Londoño, Fernando (2004). "Los Delitos Informáticos en el Proyecto de Reforma en Actual Trámite Parlamentario". *Revista de Derecho Informático*, Nº 4, mayo de 2004, pp. 171-190.

Maturana Miquel, Cristián (2002). "Responsabilidad de los proveedores de acceso y de contenido en internet". *Revista Chilena de Derecho Informático*, número 1, pp. 17-30.

Matus, Jean Pierre y Ramírez, Mª Cecilia (2014). *Lecciones de Derecho Penal Chileno, Parte Especial*. 3ª edición. Santiago: LegalPublishing-Thomson Reuters. Tomo I.

Medina, Gonzalo (2008). "Algunos aspectos de la protección penal de la privacidad". En Fernández Cruz, José Ángel (Coordinador). *Estudios de Ciencias Penales. Hacia una racionalización del Derecho Penal*. Santiago: LegalPublishing, pp. 241-262.

Moscoso, Romina (2014). "La Ley 19.223 en general y el delito de hacking en particular". *Revista Chilena de Derecho y Tecnología*, Vol 3 N° 1.

Muñoz Conde, Francisco (2015). *Derecho Penal, Parte Especial.* 20ª edición. Valencia: tirant lo blanch.

Rodríguez, Eduardo (2003). "El correo electrónico". *Revista Chilena de Derecho Informático*, número 3. Disponible en: http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewArticle/10668/11414 [fecha de visita: 30 de noviembre de 2015], s/n° de página.

Romeo Casabona, Carlos María (2002). "La protección penal de los mensajes de correo electrónico y de otras comunicaciones de carácter personal a través de internet". *Derecho y Conocimiento*, vol. 2, pp. 123-149.

Schuster, Frank Peter (2010). "IT-gestützte interne Ermittlungen in Unternehmen – Strafbarkeitsrisiken nach den §§ 202a, 206 StGB". *Zeitschrift für Internationale Strafrechtsdogmatik*, 2010, vol. 12/2015, pp. 68-75.

Ugarte Cataldo, José Luis (2011). "Privacidad, trabajo y derechos fundamentales", *Estudios Constitucionales*, Año 9, Nº 1, pp. 13-36.

Jurisprudencia citada

Tribunal Constitucional. 29 de enero de 2014. Rol N° 2379-13-INA. Disponible en: https://www.camara.cl/sala/verComunicacion.aspx?comuid=10871 [fecha de visita: 15 de noviembre de 2015].

Tribunal Constitucional. 11 de septiembre de 2011. Rol N° 2153-11-INA. Disponible en: http://www.tribunalconstitucional.cl/wp/wp-content/uploads/Rol-N-2153-correos-electr%C3%B3nicos-a-firma.pdf [fecha de visita: 15 de noviembre de 2015].

Corte Suprema. 20 de marzo de 2013. Rol N° 3951-2012. "C/ Sergio Valenzuela Cruz y otros". No disponible en colecciones físicas o electrónicas.

Corte de Apelaciones de Valparaíso. 22 de octubre de 2010. Rol N° 504-2010. No disponible en colecciones físicas o electrónicas.

Cuarto Tribunal de Juicio Oral en lo Penal de Santiago. 2 de septiembre de 2009. RIT 135-2009, RUC 0700879841-3. No disponible en colecciones físicas o electrónicas.