

La expectativa razonable de privacidad en el derecho disciplinario: aplicaciones de mensajería instantánea y jurisprudencia de la Contraloría General de la República.

The reasonable expectation of privacy in disciplinary law: instant messaging applications and the case law of the office of the Comptroller General of the Republic

*Luis Alejandro Aranda Gahona**

RESUMEN

El presente trabajo examina la jurisprudencia administrativa de la Contraloría General de la República relativa a la incorporación, -en procedimientos disciplinarios incoados en la Administración-, de mensajes provenientes de programas de mensajería instantánea como WhatsApp o Telegram. A partir del análisis de un conjunto de dictámenes que abordan la problemática, se sostiene, que el Órgano Contralor, no ha construido una regla única sobre la materia, sino que, por el contrario, sus pronunciamientos dan cuenta de diversos criterios que atienden, entre otros contextos, a quién aporta el mensaje, o cómo se accedió a su contenido. El estudio incorpora además un análisis a la sentencia de la Corte Suprema de Estados Unidos, *Katz v. United States*, con el objeto de precisar el origen de la teoría de la expectativa razonable de privacidad, como una herramienta conceptual útil para resolver este tipo de casos.

Palabras clave: Privacidad, sumario, prueba, WhatsApp, contraloría.

ABSTRACT

This article examines the administrative case law of the Office of the Comptroller General of the Republic concerning the incorporation, in disciplinary proceedings initiated within the Administration, of messages originating from instant messaging applications such as WhatsApp or Telegram. Based on the analysis of a set of rulings addressing this issue, it argues that the Comptroller has not developed a single rule on the matter. Rather, its decisions reveal a range of criteria that take into account, among other considerations, who submits the message and how access to its content was obtained. The study also includes an analysis of the United States Supreme Court's decision in *Katz v. United States*, with the aim of clarifying the origins of the reasonable expectation of privacy doctrine as a useful conceptual tool for resolving this type of case.

* Licenciado en Ciencias Jurídicas y Sociales, Universidad de Concepción. Magister en Derecho Ambiental, Universidad de Chile. Profesor de Derecho Administrativo, Universidad Autónoma de Chile. Correo electrónico: laranda@udec.cl

Fecha de recepción: 04/05/2026.

Fecha de aceptación: 12/07/2026.

Keywords: Privacy, disciplinary proceedings, evidence, WhatsApp, Comptroller's Office.

1. Introducción

La progresiva digitalización de las comunicaciones personales, laborales e institucionales ha implicado que un número significativo de interacciones entre funcionarios públicos se genere y aloje diariamente en soportes digitales y en plataformas de mensajería instantánea, tales como WhatsApp o Telegram.

En efecto, mucha información institucional y útil para el desempeño de la función pública circula por estos medios electrónicos de manera inmediata, lo que agiliza considerablemente la comunicación entre funcionarios públicos, así como el traspaso de información relevante para el cumplimiento de los fines del servicio.

Sin embargo, junto con simplificar la comunicación, este tipo de tecnologías ha complejizado profundamente las concepciones tradicionales de privacidad, confidencialidad y prueba, impactando de manera directa en el ejercicio de la potestad disciplinaria de la Administración. De esta forma, esta última se ve constantemente enfrentada a diversos cuestionamientos al momento de utilizar tales soportes como medios probatorios en procedimientos disciplinarios orientados a investigar la eventual infracción de deberes, obligaciones o prohibiciones funcionarias.

En este contexto, la naturaleza del soporte informático, la titularidad de los dispositivos o de los servicios de mensajería empleados, así como las personas que han accedido a la información transmitida por medios digitales y el modo en que dicho acceso se ha producido, se erigen, entre otros elementos, como factores relevantes para determinar si los medios de prueba obtenidos a partir de tales aplicaciones pueden ser admitidos como válidos en los referidos procedimientos disciplinarios, con el objeto de reconstruir hechos que, con frecuencia, no cuentan con otros medios directos de acreditación. Tal es el caso, por ejemplo, de conductas constitutivas de acoso laboral o sexual.

Luego, el concepto de expectativa razonable de privacidad ha adquirido especial relevancia en instancias tanto judiciales como administrativas, revelando que no nos encontramos únicamente ante un problema tecnológico, sino también frente a la necesidad de determinar en qué condiciones el ordenamiento jurídico y los operadores jurídicos reconocerán una protección efectiva de la privacidad, y en cuáles, por el contrario, aun existiendo una expectativa subjetiva de hallarse ante una comunicación privada, su contenido podrá ser expuesto y valorado en un procedimiento judicial o administrativo.

En este sentido, tanto la Contraloría General de la República en sus dictámenes, -que constituyen la fuente de estudio principal de este trabajo-, así como los tribunales superiores de justicia, han debido pronunciarse reiteradamente sobre la licitud y eficacia probatoria de conversaciones digitales obtenidas en diversos contextos, sin que se advierta una aplicación homogénea de la teoría de la expectativa razonable de privacidad, lo que ha dado lugar a criterios divergentes.

Ahora bien, cabe aclarar que lo que se aborda en el presente artículo, dice relación con la incorporación, -en sede administrativa-, de reproducciones de capturas de pantalla, imágenes, audios, o texto, que fueron enviados por medio de aplicaciones de mensajería instantánea, debiendo advertir al lector que lo que suele acompañarse en la práctica, no es el original del mensaje, toda

vez que este último es un archivo informático en un formato especial, que se encuentra alojado en el dispositivo de que se trate, sea un teléfono celular, un computador, una nube, etc. (García Mescua, 2018, p. 40).

La anterior circunstancia resulta especialmente relevante en la actualidad, debido a la facilidad con que puede presentarse prueba adulterada, como ocurre con un mensaje editado maliciosamente (se edita lo que el otro dijo mediante la alteración del código de una página web, por ejemplo), una clonación de voz, una fotografía hecha con inteligencia artificial, u otras formas de manipulación digital.

Sin embargo, en materia de procedimientos disciplinarios, Chile no cuenta con un sistema probatorio de regla tasada, donde un documento electrónico pudiera tener un valor probatorio versus una captura de pantalla que supuestamente reproduce ese contenido.

En efecto, el artículo 35 de la ley N° 19.880, aplicable supletoriamente a estos procesos, indica que los hechos podrán acreditarse por cualquier medio admisible en derecho, apreciándose en conciencia, lo que, sin perjuicio de que algún sector de la doctrina lo asimila a la sana crítica, y otro lo entiende como un sistema de valoración diferente del primero, ciertamente otorga más flexibilidad al juzgador que un sistema de prueba tasada (Isensee Rimassa, 2018, p. 55).

Puntualizado lo anterior, el presente artículo analiza la jurisprudencia de la Contraloría General de la República en la materia, con la intención de entregar una visión general de cómo dicho Órgano de Control ha resuelto situaciones en que se ha planteado la incorporación de estos medios de prueba. Ello, por estimarse necesario un trabajo con este enfoque, el que viene a sumarse a otros que ya lo han abordado, pero fundamentalmente a la luz de la jurisprudencia judicial (Roco Lehyt, 2022).

2. El fallo Katz y su evolución

Para comprender el concepto de expectativa razonable de privacidad, -concepción que posteriormente será utilizada tanto por tribunales norteamericanos, como chilenos (Escobar Veas, 2023, p. 7)-, es necesario remontarse a los Estados Unidos de la década de 1967, época en la que el FBI investigaba a Charles Katz por transmitir información vinculada a apuestas desde Los Ángeles hacia Miami y Boston mediante una cabina telefónica pública, conducta que se encontraba prohibida por la legislación federal.¹

En efecto, el título 18, sección 1084 del United States Code (18 U.S.C. § 1084), norma federal conocida como Wire Act, sancionaba la transmisión interestatal de apuestas o de información destinada a posibilitarlas, estableciendo, en lo que interesa: « *Toda persona dedicada al negocio de las apuestas o el juego que, a sabiendas, use un medio de comunicación por cable para la transmisión en el comercio interestatal o extranjero de apuestas o de información que ayude a efectuar apuestas sobre cualquier evento o competencia deportiva, o para la transmisión de una comunicación por cable que dé derecho al receptor a recibir dinero o crédito como resultado de apuestas, o de información que ayude a efectuar apuestas, será sancionada con multa de no más de 10.000 dólares o con prisión de no más de dos años, o ambas. (b) Nada de lo dispuesto en esta*

¹ Disponible en: <https://supreme.justia.com/cases/federal/us/389/347/>

sección se interpretará en el sentido de impedir la transmisión en el comercio interestatal o extranjero de información para su uso en la información noticiosa sobre eventos o competencias deportivas, ni la transmisión de información que ayude a efectuar apuestas sobre un evento o competencia deportiva desde un Estado donde esas apuestas sean legales hacia un Estado donde también lo sean. »

Luego, el FBI sintiéndose validado por la jurisprudencia vigente hasta ese entonces en la materia, procedió, sin una orden judicial, a la instalación de un sistema de intervención consistente en escucha y grabación en el exterior de la cabina telefónica donde Katz realizaba sus llamadas, a objeto de obtener la prueba necesaria para detenerlo y llevarlo a juicio, lo que efectivamente logró.

En dicho contexto, el Tribunal del Distrito Sur de California conoció de la acusación deducida por diversos cargos contra Katz, quien alegó que la actividad de vigilancia e interceptación desarrollada por el gobierno había lesionado la esfera de privacidad en la que razonablemente confió al utilizar la cabina telefónica. A su juicio, la actuación de los agentes configuraba un registro e incautación incompatible con la Cuarta Enmienda de la Constitución de los Estados Unidos, toda vez que se había ejecutado sin contar con una orden judicial previa, exigida constitucionalmente para este tipo de injerencias.

Recordemos que la Cuarta Enmienda protege a las personas frente a incautaciones y registros irrazonables por parte de agentes del Estado, indicando que: *«No se violará el derecho del pueblo a la seguridad de sus personas, hogares, documentos y pertenencias, contra allanamientos e incautaciones fuera de lo razonable, y no se expedirá ningún mandamiento judicial para el efecto, si no es en virtud de causa probable, respaldada en juramento o promesa, y con la descripción en detalle del lugar que habrá de ser allanado y de las personas o efectos que serán objeto de detención o incautación.»*²

Ahora bien, hasta ese entonces, el año 1967, la protección de la Cuarta Enmienda, estaba lógicamente más asociada a incautaciones y registros físicos que a medios electrónicos, circunstancia que se reflejaba en la jurisprudencia vigente en Estados Unidos, así como la confianza del FBI en que su actuar no sería cuestionado.

Con todo, el tribunal desestimó tal argumentación, razonando que no había existido penetración física en la cabina telefónica mientras era ocupada por el acusado, por lo que no se verificaba infracción alguna a la Cuarta Enmienda.

Entonces, el caso llegó a la Corte Suprema de los Estados Unidos, instancia en la que Charles Katz planteó que la cuestión consistía en determinar si:

- Una cabina telefónica pública, era un área constitucionalmente protegida de modo que la prueba presentada por el FBI, obtenida mediante la instalación de este dispositivo de escucha y grabación, violaba el derecho a la privacidad de quien usa esa cabina; y
- Si resulta imprescindible una penetración física en un área constitucionalmente protegida, para estimar que existe un registro e incautación que vulnere la Cuarta Enmienda.

² <https://www.state.gov/wp-content/uploads/2020/05/SPA-Constitution.pdf>

La Corte Suprema de los Estados Unidos, observando que las partes en el juicio le atribuían gran importancia a la calificación jurídica de la cabina telefónica, indicó que dicho planteamiento desviaba la atención del problema, pues la Cuarta Enmienda protege a las personas no a los lugares, indicando que lo que una persona expone conscientemente al público, aun en su propio hogar, u oficina, no es objeto de protección de dicha enmienda, pero aquello que procura mantener en privado, incluso en un área accesible al público, sí puede estar constitucionalmente protegido.

Incluso el FBI, para reafirmar que la cabina no podía ser un área constitucionalmente protegida, subrayaba el hecho de que estaba construida parcialmente de vidrio, de modo que, una vez dentro, la persona era tan visible como si hubiera permanecido afuera de ella, argumento que la corte desestimó.

En efecto, los jueces estimaron que quien ocupa la cabina, cierra la puerta detrás de sí, y paga la tarifa que le permite efectuar la llamada, ciertamente puede suponer que las palabras que pronuncia en el auricular no serán difundidas al mundo.

La Corte Suprema, por tanto, dio la razón a Katz, destacando especialmente la opinión concurrente del juez Harlan, cuyo razonamiento dio origen al concepto de expectativa razonable de privacidad.

Para él, si se quiere determinar si en una situación procede la protección dispensada por la Cuarta Enmienda, había que formular un test integrado por dos requisitos copulativos: primero, que el individuo hubiese exteriorizado una expectativa real (subjetiva) de privacidad; y, segundo, que dicha expectativa fuese una que la sociedad estuviese dispuesta a reconocer como razonable.

En tal sentido, advertía que el domicilio de una persona constituye, por regla general, un ámbito en el que existe una legítima expectativa de privacidad. Al contrario, respecto de aquellos objetos, actividades o manifestaciones que el individuo expone a terceros, no cabe reconocer protección constitucional, en la medida en que no ha existido una voluntad de sustraerlos del conocimiento ajeno.

Bajo la misma lógica, las conversaciones desarrolladas en espacios abiertos no quedarían amparadas frente a su eventual conocimiento por terceros, toda vez que, en tales circunstancias, la expectativa de privacidad no puede reputarse razonable.

La relevancia de este caso radica en que desplazó la comprensión tradicional que condicionaba la protección de la Cuarta Enmienda a la existencia de una invasión física del espacio. A partir de entonces, se abrió paso una concepción más amplia entendiendo que una expectativa razonable de privacidad podría ser vulnerada tanto por invasiones físicas como electrónicas.

Esta teoría, ampliamente utilizada con posterioridad por los tribunales estadounidenses y estructurada sobre la base de los dos requisitos ya referidos, fue más tarde objeto de crítica por parte del profesor de derecho Orin Kerr, quien, a partir de una investigación empírica sobre jurisprudencia de ese país, sostuvo que, en la práctica, el criterio se había deformado hasta el punto de que el elemento subjetivo había caído en el olvido y había dejado, en los hechos, de ser aplicado, transformándose en una verdadera «doctrina fantasma» (Kerr, 2015).

Según explica Kerr, el elemento subjetivo no aludía originalmente tanto a lo que la persona sintiera internamente acerca de su privacidad, sino más bien a aquello que exteriorizaba, esto es, a las

conductas mediante las cuales manifestaba su intención de mantener determinado ámbito dentro de su esfera privada. Sin embargo, sostiene, la jurisprudencia norteamericana posterior tendió a reinterpretar este aspecto como una cuestión referida a si la persona «esperaba» privacidad, desdibujando así su sentido original. Como consecuencia de ello, el elemento objetivo pasó a ocupar el lugar decisivo, reduciéndose el análisis, en la práctica, a la pregunta de si la sociedad está dispuesta a reconocer esa expectativa de privacidad como razonable.

Finalmente, Kerr propone reconocer expresamente esta evolución y sincerar el estado actual de la doctrina, planteando que la teoría formulada a partir de Katz habría quedado en desuso en su versión originaria de dos pasos —subjetivo y objetivo—, subsistiendo en los hechos como un test de una sola etapa, el objetivo.

3. La jurisprudencia de la Contraloría General de la República sobre mensajería instantánea y prueba en denuncias y procedimientos disciplinarios

A continuación, procederemos a estudiar la jurisprudencia administrativa de la Contraloría General de la República, en la cual se analiza la procedencia de incorporar prueba consistente en mensajes, texto, imágenes o audios enviados a través de aplicaciones o programas de mensajería instantánea.

Recordemos que el artículo 6° de la ley N° 10.336, establece que al Contralor General le corresponderá de forma exclusiva informar sobre, entre otras materias, los asuntos que se relacionen con el Estatuto Administrativo y con el funcionamiento de los Servicios Públicos sometidos a su fiscalización, todo ello para los efectos de la correcta aplicación de las leyes y reglamentos que los rigen.

Finaliza el artículo, indicando que solo las decisiones y dictámenes del Ente Contralor, serán los medios que podrán hacerse valer como constitutivos de la jurisprudencia administrativa.

Cabe advertir, que el presente estudio, comprende solo dictámenes del Ente Contralor, sin abarcar resoluciones y oficios, por ejemplo, de sus oficinas regionales, u otras reparticiones que no crean jurisprudencia, sino que solo la aplican³.

3.1. La prevención preliminar: Los programas de mensajería instantánea como WhatsApp no son los canales idóneos para impartir instrucciones institucionales

Aunque la línea jurisprudencial que se expondrá en este acápite no aborda directamente el problema de la expectativa razonable de privacidad, ni la ilicitud de una prueba obtenida sin el consentimiento de su emisor, -lo que examinaremos más adelante-, su estudio resulta igualmente valioso, pues permite conocer el criterio del Ente Contralor, acerca del rol que ocupan las aplicaciones de mensajería instantánea en el ejercicio de la Función Pública.

Dictamen N° 35.523, de 2016

³ Aun cuando sería sumamente valioso contar con la posibilidad de conocer y estudiar cómo dichas dependencias no dictaminadoras aplican dichos pronunciamientos a casos concretos, éstos no se encuentran disponibles en la base electrónica de dictámenes de la Contraloría General de la República.

El caso se originó a partir del reclamo presentado por un funcionario de Gendarmería de Chile, quién alegó que esa institución ignoró una denuncia de acoso laboral deducida en contra de otro empleado por enviarle una instrucción de servicio a través de WhatsApp, mientras se encontraba en calidad de franco.

En este pronunciamiento, la Contraloría parte puntualizando que el uso de medios tecnológicos como teléfonos celulares u otras herramientas de las tecnologías de la información, pueden servir de apoyo en el ejercicio de la función pública, en cuanto constituyen una manifestación de los principios de eficiencia y eficacia que rigen dicha labor.

Sin embargo, precisa, enviar mensajes al teléfono celular personal de un funcionario para impartirle instrucciones institucionales no constituye una vía idónea para ello, pues dichas directrices deben ser canalizadas por medio de los canales formales del servicio, dentro de las cuales no se encuentran las redes sociales.

Dictamen N° 36.110, de 2017

El anotado criterio es reiterado posteriormente en un pronunciamiento que resuelve un reclamo de un ex funcionario de Carabineros de Chile, a quien se le reprochó no contestar llamadas efectuadas a su teléfono particular, ni mensajes que se le remitieron a su WhatsApp.

En este caso, la Contraloría General resolvió que «no procede utilizar la red social WhatsApp para impartir instrucciones relativas al desempeño laboral de un funcionario, pues corresponde que las directrices sean canalizadas, como se expresó, a través de los mecanismos institucionales, dentro de los que no se advierte se contemplen las distintas redes sociales de uso particular».

Dictamen N° 7.849, de 2020

En esta ocasión, se trató de una solicitud efectuada por Carabineros de Chile, para que la Contraloría reconsiderara su criterio acerca de la utilización de WhatsApp como medio para citar e impartir instrucciones a sus funcionarios cuando existan situaciones de anormalidad en que se requiere una intervención rápida de todo el personal disponible para reestablecer y/o asegurar el orden y la seguridad pública⁴.

Al respecto, la Contraloría General, señala que «las comunicaciones a los servidores de un determinado organismo público se deben realizar a través de los medios y mecanismos institucionales, sin que sea exigible a los respectivos funcionarios disponer de un bien de su patrimonio, como es el caso de un teléfono móvil particular para tal efecto».

A continuación, el Ente Contralor concluye:

«...en concordancia con los citados principios de eficiencia y eficacia, es menester considerar que para efectos de afrontar las contingencias por las que se consulta, Carabineros de Chile puede utilizar la red social whatsapp para canalizar directrices de carácter institucional al teléfono móvil

⁴ Cabe indicar que la fecha del dictamen citado corresponde al 15 de abril de 2020, época en que el país atravesaba dos hechos de alta conmoción nacional, esto es, el estallido social de octubre de 2019 y la pandemia mundial COVID-19.

particular del personal institucional, relativo a su desempeño, en la medida que el respectivo funcionario haya registrado voluntariamente dicho equipo para tales fines y ello no le signifique un detrimento patrimonial.»

Respecto de este pronunciamiento, debe subrayarse que la Contraloría señala expresamente que viene a complementar los dictámenes antes citados, por lo que no los deja sin efecto, ni tampoco los reconsidera, constituyendo una autorización especial, para una institución en particular, respecto de circunstancias específicas, con los requisitos y contextos que allí se indican.

3.2. La Protección de comunicaciones privadas frente a terceros no autorizados, incluso en computadores institucionales

Dictamen N° 74.351, de 2011

Se trató de un pronunciamiento sobre la aplicación de la medida de destitución como resultado de un procedimiento disciplinario incoado en contra de dos funcionarias municipales, al haberse detectado, mediante una revisión general de los computadores del municipio, que en sus equipos existían programas instalados que no guardaban relación con sus funciones, y que además empleaban el software de chat Microsoft Messenger.

En ese contexto de chequeo general, las funcionarias acusaron que se habría accedido al contenido de sus conversaciones en ese programa, por lo cual interpusieron una querrela criminal por el delito de violación de correspondencia, violación de respeto y protección de la vida privada, mediante captación, grabación y reproducción sin autorización de esas comunicaciones privadas, esto es, desde el programa Messenger instalado en sus computadoras institucionales.

Ahora bien, en relación con la forma en que se obtuvieron las conversaciones privadas sostenidas por las acusadas, la Contraloría señaló:

«Con todo, resulta menester hacer presente que, atendido que las comunicaciones a que se ha hecho referencia se efectuaron a través de un sistema de mensajería instantánea asociado a una casilla de correo privada, no resultó procedente, en razón de lo prescrito en el artículo 19 N°s. 4 y 5 de la Carta Fundamental, la actuación de determinados servidores municipales de acceder al contenido de las conversaciones privadas sostenidas por otros empleados de la Municipalidad de Concón a través de medios electrónicos, sin el consentimiento de éstos.»

Lo interesante del caso, en mi opinión, radica además en que el Ente Contralor no se distrajo en que Messenger estuviera instalado en los computadores institucionales, sino que centró su análisis y conclusión respecto del acceso de terceros al contenido de mensajes privados.

Dictamen N° 10.352, de 2019

Se trató de un procedimiento disciplinario instruido por la Policía de Investigaciones de Chile, en contra de uno de sus funcionarios destinados a labores de extranjería y policía internacional en el Aeropuerto de Santiago, a quien se le atribuyó haberse referido con vocabulario y términos inapropiados en contra de una superior jerárquico en el contexto de una conversación sostenida a través de WhatsApp con una tercera persona. El contenido de dicha comunicación habría sido visto por otros miembros de la institución, al momento de abrir la versión web de dicha aplicación en un computador fiscal ubicado a la vista del público.

En este caso, la Entidad de Control estimó que no constaba en el proceso que los partícipes de la conversación sostenida a través de WhatsApp hubieran permitido que terceros a quienes los mensajes no iban dirigidos, accedieran a su contenido. Sobre ese razonamiento, equiparó dicha vulneración, a la obtención clandestina y subrepticia de una conversación telefónica.

Finalmente, objetó la sanción sosteniendo que se fundamentó en una prueba obtenida por medios ilícitos, importando una vulneración relevante al debido proceso.

3.3. Autoría, veracidad y fiabilidad

Dictamen N° 13.520, de 2017

El pronunciamiento se produce en el contexto de un sumario administrativo sustanciado en la Dirección Regional de Obras Portuarias, de la Región de Aysén para investigar las eventuales responsabilidades administrativas involucradas en la entrega a personas externas del servicio, vía correo electrónico, de información privilegiada y reservada en relación con procesos de licitación del referido organismo. Asimismo, se indagó la existencia de eventuales sobornos conforme a evidencia obtenida desde mensajes de WhatsApp.

Al respecto, la Contraloría General de la República, conociendo del caso vía toma de razón, se pronunció sobre la legalidad de la medida disciplinaria de destitución impuesta al inculpado, quien la impugnó arguyendo que el procedimiento adolecía de vicios que incidían en su validez.

En su dictamen, el Órgano de Control, indicó que la medida de destitución exige un estándar de tal rigurosidad, que para que ésta pueda ser aplicada, es exigible que del mérito del proceso aparezca indubitada e irrefutablemente, que los hechos se encuentran plenamente probados, lo que estimó, no ocurría en el caso.

Respecto de las conversaciones de WhatsApp, la Contraloría desestimó su valor probatorio al sostener, derechamente, que no se demostró la veracidad de ellas, ni tampoco la fecha en que se habrían producido, lo que comprometía el derecho a defensa del afectado.

En relación con los correos electrónicos que sirvieron de prueba para sancionar al funcionario, el Ente Contralor, objetó la falta de diligencias orientadas a determinar si dichos mensajes habían sido efectivamente enviados por el inculpado.

En este punto, la Contraloría tomó en consideración que, durante la etapa indagatoria del sumario en estudio, varios testigos habían declarado que la clave del computador del inculpado era conocida por otros servidores, e incluso que uno de ellos, precisamente, quien acompañó los mensajes que dieron origen al procedimiento disciplinario, tenía la costumbre de ingresar a los computadores de otros empleados del servicio.

Sobre esa base, concluyó que no existía certeza que el inculpado fuera el autor del correo electrónico y las conversaciones por WhatsApp.

Por consiguiente, establece que, si se comprueba que otras personas pudieron acceder a los dispositivos del inculpado, este hecho resta valor probatorio a ese tipo de comunicaciones, pues no consta fehacientemente la autoría de ellos.

Dictamen N° 1.127, de 2021

En el contexto de la pandemia mundial de COVID-19, la Contraloría recibió una solicitud parlamentaria para que emitiera un pronunciamiento jurídico sobre la conducta del entonces Intendente de la Región de los Lagos, el cual habría comunicado antes que a la comunidad regional, mediante WhatsApp a un grupo de ganaderos de la ciudad de Osorno, que se decretaría la medida sanitaria de cuarentena, lo que, de acuerdo con el requerimiento, configuró uso de información privilegiada, vulnerando así el principio de probidad administrativa.

Al respecto, el análisis de la Entidad de Control se centró en que, aunque circulaba una fotografía de un mensaje que habría sido enviado por el intendente en un grupo de WhatsApp, no aparecía el día en que habría sido expedido, por lo que no era posible acreditar que dicho mensaje hubiera sido expedido por el Intendente en el día y hora denunciada.

Lo relevante de este pronunciamiento, radica en que el problema central no se desplazó a la privacidad del mensaje ni cómo se obtuvo, sino en la falta de fiabilidad sobre su autoría y su fecha de envío.

3.4. Mensajes aportados por los propios intervinientes**Dictamen E288163, de 2022**

Ante un incremento sostenido de denuncias por acoso laboral y sexual, que acompañaban capturas de pantalla o audios enviados a través de aplicaciones de mensajería instantánea como WhatsApp o Telegram, la Unidad de Protección de Derechos Funcionarios de la División Jurídica de la Contraloría General, solicitó un pronunciamiento jurídico sobre la posibilidad de que esos mensajes pudieran ser presentados como medios de prueba por uno de los intervinientes de esa conversación.

En dicho pronunciamiento, la Entidad de Control, aplicando supletoriamente el artículo 35 de la ley N° 19.880, -conforme a la cual los hechos relevantes para la decisión de un procedimiento pueden acreditarse por cualquier medio de prueba admisible en derecho-, sostuvo que los fiscales instructores se encuentran facultados para valorar los audios o capturas de pantalla de conversaciones, mensajes o imágenes de redes sociales, como WhatsApp o Telegram.

Lo anterior, indica, se ve reforzada por el hecho de que el acoso laboral o sexual, no suele ocurrir en un contexto público o evidente, sino que, al contrario, se despliega en muchas ocasiones al margen de éste, por lo que un audio o captura de pantalla, puede ser uno de los pocos, o incluso el único medio al que se puede recurrir a fin de probarlos o exculpar al denunciado.

Ahora bien, en relación a la privacidad, la Contraloría General de la República señala que:

«Refuerza lo anterior el hecho de que los emisores de los mensajes, audios, participantes en conversaciones o remitores de imágenes por redes sociales no pueden tener una expectativa de confidencialidad al enviarlos, iniciarlas, subir imágenes o remitirlas a un tercero, según sea el caso, toda vez que, aun cuando aquellas acciones puedan considerarse, en algunos casos, como generadas o gestadas en un contexto de comunicación personal, el destinatario de aquellos pasa a ser un interesado incumbente de los mismos y puede hacer un uso razonable de estos, como sería

entregarlos como medios de prueba en un proceso sumarial, dado que, además, se trata de elementos que son idóneos y necesarios para tales fines.»

A continuación, concluye que los audios o capturas de pantalla de conversaciones sostenidas en redes sociales, pueden ser utilizados y valorados como medios de prueba válidos en sumarios administrativos, siempre que sean aportados por uno de los intervinientes en la recepción, envío o conversación, y que éste lo entregue voluntariamente en un proceso sumarial con dicha finalidad probatoria.

Finalmente, y un punto que resulta especialmente relevante, es que el dictamen también exige que pueda acreditarse que los mensajes se refieren o guardan relación con la presunta víctima o con el presunto victimario, vale decir, no basta que solo sea acompañado por uno de los intervinientes, sino que además debe acreditarse que guardan relación con dichas personas.

Ahora bien, si hiciéramos el ejercicio de reconstruir el razonamiento del Juez Harlan, respecto de este dictamen, podríamos desglosar el razonamiento de la siguiente forma:

- El mensaje, audio, o texto, es enviado deliberadamente a otro, de manera que su emisor exterioriza su contenido frente a esa persona, y por lo mismo, no lo mantiene reservado respecto de ella.
- En tal contexto, la expectativa razonable de privacidad no resultaría oponible al tercero para estimar que no pueda utilizarlo en contra del emisor como prueba en un procedimiento disciplinario.

3.5. Casos de mensajes y publicaciones con menor protección de privacidad

Aunque dos de las hipótesis y controversias que se exponen a continuación dicen relación con publicaciones efectuadas en Facebook, -las cuales no son completamente equivalentes a los mensajes enviados por aplicaciones de mensajería instantánea a las que nos hemos referido anteriormente-, creo importante detenernos brevemente en este tipo de casos, a objeto de conocer el criterio de la Contraloría General de la República, cuando el contenido, aun cuando se generó en un contexto cerrado, termina siendo conocido por un número indeterminado de personas.

Dictamen 44.894, de 2014

Se trató de un sumario administrativo, donde se investigó la eventual responsabilidad administrativa de un funcionario del Servicio de Registro Civil e Identificación, por haber escrito comentarios inapropiados en Facebook respecto de otros servidores.

En dicho caso, se defendió que los comentarios publicados en la red social Facebook, correspondían al ámbito de las comunicaciones privadas, y que además constituían opiniones personales amparadas en la libertad de expresión, por lo que no pueden ser objeto de una sanción administrativa. Sin embargo, el argumento fue desestimado por el Ente Contralor, el cual afirmó que:

«En relación con lo anterior, es necesario expresar que si bien la mencionada red social no es un sistema de libre acceso, lo cierto es que las descalificaciones ahí vertidas fueron conocidas por un

gran número de individuos, entre los cuales se encuentran varios empleados del servicio, hecho que quedó demostrado con las declaraciones prestadas en el curso de la indagatoria, de lo que es dable inferir que la citada conducta constituye una infracción a la prohibición contemplada en el artículo 84, letra l), de la ley N° 18.834, al constituir un acto atentatorio a la dignidad de otro funcionario.

Finalmente, en lo que dice relación con la anotada garantía, esto es, el derecho de libre expresión, -en que se pretende amparar el actuar del implicado trabajador-, se debe hacer presente que ella tiene que ejercitarse con respeto y no puede significar menoscabar la dignidad de terceras personas.»

Dictamen 13.606, de 2018

Se trató de un sumario instruido en contra de una funcionaria de Carabineros de Chile, a quien también se le atribuyó haber realizado comentarios en contra de otros funcionarios de la institución, a través de Facebook.

Al respecto, la Contraloría estimó procedente la incorporación al expediente de fotocopias simples de los comentarios vertidos en la red social, indicando que:

«Seguidamente, sobre el hecho de haber incorporado en el expediente disciplinario fotocopias simples de los comentarios que la afectada realizó en su cuenta de facebook, los que correspondería al ámbito de las comunicaciones privadas de aquella, se debe expresar, en armonía con lo sostenido en el dictamen N° 44.894, de 2014, de este origen, que si bien la mencionada red social no es un sistema de libre acceso, lo cierto es que las expresiones ahí vertidas -en contra de personal de Carabineros de Chile, que participó en una comida de despedida-, fueron conocidas por varios funcionarios de esa institución, lo que quedó comprobado en el curso de la indagación de que se trata, por lo que no se aprecia algún impedimento para haber incorporado tales documentos, considerando que la citada conducta reprochada implicó un acto atentatorio contra la dignidad de otros funcionarios.»

Dictamen E155404, de 2021

Este pronunciamiento, tuvo su origen en la denuncia efectuada por un grupo de parlamentarios en contra de una ministra, a quién se le acusaba haber impartido vía WhatsApp, instrucciones orientadas a favorecer la candidatura de su pareja, con un eventual uso de recursos públicos, todo ello basado en un reportaje emitido por un canal de televisión.

Requerido su informe, la secretaría de Estado, indicó que se trató de conversaciones en el marco del ámbito privado y de confianza, por lo que no podían ser utilizadas por haber sido obtenidas por medios ilícitos, sin el consentimiento de sus partícipes.

Además, indicó que ese ministerio no contaba con una cuenta institucional de WhatsApp, por lo que las conversaciones expuestas en el reportaje corresponden a un grupo particular, que se encuentra integrado tanto por personas que se desempeñaban en el ministerio, como otras ajenas a él, por lo que la utilización de ese canal privado no puede considerarse dentro de actividades laborales desarrolladas por funcionarios.

Ahora bien, al resolver sobre la procedencia de considerar los mensajes para examinar la conducta denunciada, se concluyó:

«En relación con la materia y de manera preliminar, sobre la falta de consentimiento de los funcionarios que participaban de los grupos de WhatsApp que se mencionan en el reportaje, para que se conocieran por terceros las conversaciones mantenidas en estos y que fundaron la denuncia que se examina, corresponde aclarar que se trata de conversaciones vía WhatsApp que, fruto del reportaje emitido con fecha 17 de octubre de 2021 por un canal de televisión que las difundió, trascendieron a la opinión pública y son hechos públicos y notorios.»

Vale decir, el hecho de que los mensajes hayan sido ampliamente difundidos por medios de prensa a nivel nacional, llevó al Ente Contralor a considerarlos hechos públicos y notorios, por lo que no cuestionó la manera en que dichos mensajes fueron obtenidos y presentados.

4. El fallo de la Corte de Apelaciones de Copiapó

Antes de continuar, resulta conveniente detenerse, en una sentencia que generó bastante cobertura tanto en prensa, redes sociales y foros especializados, y que se encuentra directamente relacionada con la problemática analizada en el presente artículo, y cuyo análisis además nos permitirá posteriormente visualizar claramente la metodología que debe aplicarse para ejecutar el test del fallo Katz vs United States.

Se trató de un recurso de protección interpuesto por un funcionario de Carabineros de Chile, en contra de otra servidora de dicha institución que accedió a una conversación sostenida entre el recurrente y un tercero, a través de WhatsApp Web, el cual se encontraba instalado en un computador institucional.

El conflicto surge porque la recurrida, en el cumplimiento de sus funciones, utilizó el computador institucional compartido, en el cual se encontraba abierta la sesión de WhatsApp Web del recurrente, advirtiéndolo en la única conversación visible, que se hacía referencia a su nombre y de otro funcionario, por lo cual informó de ello a su jefatura.

La Corte rechazó el recurso interpuesto por el funcionario, poniendo especial énfasis en que el computador era de uso compartido, así como también en que el propio recurrente declaró que hace meses sabía que su sesión se encontraba abierta en un dispositivo desconocido, además que había advertido que ciertos mensajes aparecían como leídos en su WhatsApp, antes de que él mismo los viera, sin que ello, motivara alguna conducta de resguardo, por lo que el tribunal estimó que el actor había consentido de manera tácita a que terceros accedieran al contenido de esa aplicación de mensajería.

El fallo fue posteriormente confirmado por la Corte Suprema.

5. Propuesta metodológica para el análisis de mensajes de mensajería instantánea en procedimientos disciplinarios

A partir de la jurisprudencia administrativa recientemente analizada, es posible proponer un método de referencia basado en preguntas, no secuenciales, que se responden a partir de los criterios que sustenta la Contraloría General de la República en cada uno de los pronunciamientos señalados, intentando además conjugar alguno de ellos con la teoría de la expectativa razonable de privacidad en los términos del fallo Katz vs United States, y en especial, la concurrencia del juez Harlan.

5.1. ¿El mensaje lo aporta un interviniente o un tercero?

Este criterio, descansa sobre la idea de analizar la procedencia de incorporar como medio de prueba en un procedimiento disciplinario una captura de pantalla, una imagen, audio o texto proveniente de aplicaciones de mensajería instantánea, y consiste en determinar quién está intentando incorporarlo al proceso. En dicho contexto cabe distinguir si nos encontramos frente a uno de los intervinientes en la respectiva conversación o frente a un tercero ajeno a ella.

En la primera de las hipótesis, vale decir, cuando uno de los intervinientes de la conversación pretende aportar el material al procedimiento, no se advierte impedimento para que lo haga, todo ello a la luz del dictamen E288163, de 2022.

Al contrario, cuando un tercero ajeno a la conversación presenta el material, y éste no fue obtenido con el consentimiento de su emisor o destinatario, la prueba queda expuesta a ser declarada como ilícita. En apoyo de esta conclusión, encontramos el dictamen N° 10.352⁵.

Por tanto, la expectativa razonable de privacidad no es oponible frente al propio interlocutor del mensaje para que éste lo utilice como prueba. Lo anterior, no significa en modo alguno que la comunicación pierda por completo su carácter privado frente a terceros, pues en rigor ha sido el mismo emisor del mensaje el que ha expuesto voluntariamente su contenido ante el destinatario.

Ahora bien, cabe preguntarse qué ocurre si el propio emisor, consiente en que terceros ajenos a la conversación accedan a su contenido, o no adopta las medidas adecuadas para resguardar los mensajes de la vista de terceros. El siguiente criterio sirve para dilucidar la respuesta.

5.2. ¿Cómo el tercero accedió al contenido?

Estamos frente a una situación en que el funcionario utiliza un servicio de mensajería instantánea instalado o abierto en el computador institucional ubicado en dependencias del organismo público, y un tercero accede al contenido de los mensajes, capturándolos por algún medio como podría ser fotografiándolos con un teléfono celular, o imprimiéndolo directamente desde el equipo, para luego presentarlo como medio de prueba en su contra.

En la hipótesis, la Contraloría General de la República aparece especialmente garantista, lo que resulta de analizar el criterio contenido en el dictamen N°10.352, de 2019, que rechaza la aceptación de los mensajes, aun cuando la conversación se sostuvo en un computador fiscal que se encontraba en el aeropuerto y a la vista del público⁶.

⁵ Aun cuando el dictamen E155404, de 2021, aceptó puntualmente la validez de los mensajes presentados en un reportaje de televisión, lo cierto es que el Órgano Contralor abordó argumentos que relativizaban su carácter de chat privado. Si a ello se le agrega que no se trató de evaluar la legalidad de la incorporación de un mensaje en un procedimiento disciplinario, hace concluir que no constituye una regla general que se oponga a la línea jurisprudencial ya analizada.

⁶ En el dictamen N°13.520, de 2017, la objeción de la Entidad de Control se basó en la falta de certeza en la autoría y fiabilidad del material digital, precisamente porque el computador institucional desde donde supuestamente se enviaron los mensajes, era accesible a otras personas, pero no constituye un examen a la forma en que se obtuvieron, el tipo de acceso, etc.

Ahora bien, válidamente cabe preguntarse si el referido criterio jurisprudencial se encuentra en abierta oposición o no al fallo de la Corte de Apelaciones de Copiapó en el caso del computador compartido por Carabineros.

Para responder dicha pregunta, estimo útil acudir a un razonamiento basado en las dos preguntas del fallo Katz, lo que, en el pronunciamiento del Órgano Contralor, puede reconstruirse implícitamente, aunque en una forma que coincide con la crítica del profesor Kerr.⁷

En efecto, el aludido pronunciamiento, no indaga si el afectado tomó precauciones para evitar que sus conversaciones fueran vistas por terceros, como bloquear pantalla, cerrar sesión, etc., sino que se concentra solo en el aspecto objetivo del test, al afirmar que «no puede pretenderse que sea constitutivo de un medio lícito grabar clandestina y subrepticamente una conversación telefónica -para la especie, un tipo de comunicación privada-, esto es, sin el conocimiento del emisor de las expresiones registradas en audio y que, posteriormente, tal elemento sea admitido, incorporado y valorado en el proceso disciplinario».

Ahora bien, seguir el método de Katz, implicaría, en primer lugar, analizar si esa persona utilizó algún sistema de bloqueo de pantallas, usó doble autenticación, etc., no lo que «pensó» o «sintió» en su fuero interno, sino lo que exteriorizó, aspecto en el cual el aludido pronunciamiento no profundiza.

Solamente después de constatar dicha exteriorización, corresponde formular la segunda prueba, esto es, si en el contexto de la situación planteada, resulta razonable esperar que nadie ingrese al espacio de trabajo ajeno, fuerce o burle las barreras, tanto físicas (puertas) como electrónicas (bloqueo de pantalla o uso de claves, o explorar las ventanas) hasta encontrar la información que su titular había procurado mantener fuera del conocimiento de terceros.

Por el contrario, en el fallo de la Corte de Apelaciones de Copiapó sí apreciamos una formulación más nítida del test, en cuanto dicho tribunal dirige su análisis a determinar primeramente si el funcionario había adoptado medidas concretas para resguardar su privacidad, -como cerrar la sesión abierta en otros dispositivos o desvincular accesos desconocidos-, lo que incluso puede advertirse en su considerando 9° al expresar que «a partir de esta conducta, es dable plantear, que el recurrente expuso su información, permitiendo que de un modo tácito terceros pudieran acceder al contenido de su mensajería».

Por ende, el análisis del Tribunal de Alzada, no centra su atención en lo que el funcionario hubiera pensado o sentido en su fuero interno, sino en el hecho de que no exteriorizó una conducta en la dirección de excluir el contenido de sus mensajes al conocimiento de terceros, pasando luego

⁷ Recordemos que Kerr sostiene que la pregunta formulada por el juez Harlan no estaba originalmente destinada a indagar que sentía, pensaba o esperaba internamente la persona emisora del mensaje, sino que, si éste había exteriorizado una pretensión de privacidad, como cuando se ingresaba a una cabina telefónica y se cerraba la puerta. Por ende, lo subjetivo, no era un rigor una indagación psicológica, mental, sino más bien un juicio a la conducta exteriorizada del individuo. Posteriormente, expone Kerr, la jurisprudencia norteamericana mal interpretó esa pregunta y la convirtió en una verdadera prueba subjetiva consistente en un examen de lo que la persona pensaba o esperaba (imposible), lo que vació de contenido útil el primer tramo del test y trasladó el peso decisivo del análisis al componente objetivo, vale decir, la pregunta si la sociedad está dispuesta a reconocer esa expectativa como razonable.

responder la segunda pregunta del test, al estimar que en esas circunstancias no resulta objetivamente razonable esperar una expectativa de privacidad.

Por consiguiente, el dictamen y la sentencia no son inconciliables, sino que expresan énfasis diferentes, puesto que mientras el primero centra su análisis en que no resulta posible admitir una grabación subrepticia como medio lícito de prueba, -sin indagar en el comportamiento del afectado, el fallo examina con mayor detalle el caso, abarcando tanto si el titular exteriorizó efectivamente su pretensión de privacidad, y si, en ese contexto, resultaba objetivamente razonable reconocerla.

5.3. ¿El soporte es institucional, personal o mixto?

El siguiente criterio es determinar la naturaleza del soporte utilizado, para lo cual corresponde distinguir las siguientes situaciones.

a.- El equipo es institucional, pero el servicio de mensajería no lo es

En este caso, el solo hecho de que el dispositivo sea fiscal, de acuerdo con la jurisprudencia administrativa examinada, no tiene relevancia para omitir los requisitos necesarios para presentar su contenido en un procedimiento disciplinario, como el consentimiento del afectado, protección que incluso alcanza a revisiones generales que se hagan por parte del organismo público, como ocurrió en el caso del dictamen N° 74.351, de 2011.

b.- El dispositivo y el software son institucionales

Se trata de una situación en que un tercero logra acceder a los mensajes de manera subrepticia, pues el emisor ha adoptado las precauciones correspondientes para mantener dicho material fuera del ojo de terceros.

Aunque esta hipótesis no ha sido abordada directamente por la Contraloría, el criterio sostenido en el dictamen 74.351, de 2011, permite concluir, por analogía, que la naturaleza institucional del programa de mensajería no excluye por sí sola la protección de la privacidad de los mensajes, dado que, en esa ocasión, se acreditó que al no existir correo institucional en el municipio de que se trataba, se permitía usar MSN Messenger como chat institucional, lo que no obstó a que la obtención de su contenido en una revisión efectuada por personal de la entidad edilicia, fuera objetada por el Ente de Control.

c.- El dispositivo y el software son personales

El caso se encuentra resuelto en el dictamen E288163, de 2022, puesto que dichos mensajes se dan mayoritariamente en un contexto de celulares personales y WhatsApp, por lo que cabe concluir que dicho carácter personal, no excluye la protección de privacidad que hemos analizado.

d.- El equipo es personal, pero el software es institucional

Aunque esta hipótesis no se encuentra explícitamente resuelta por la jurisprudencia administrativa, estimo que los dictámenes Nos 74.351, de 2011⁸, y 10.352, de 2019, permiten, por analogía, sostener que la circunstancia de que el contenido se soporte a través de un software institucional de mensajería instantánea no echa abajo, por sí sola, toda expectativa de privacidad ni autoriza automáticamente el acceso de terceros ajenos a la comunicación.

6. Conclusiones

La jurisprudencia administrativa analizada en este trabajo permite afirmar que la Contraloría General de la República, no resuelve mediante una regla única la posibilidad de incorporar a procedimientos disciplinarios mensajes provenientes de programas de mensajería instantánea como WhatsApp.

En dicho sentido, el Órgano de Control, distingue una serie de criterios para resolver las controversias asociadas a dicha incorporación, atendiendo en algunas oportunidades a la calidad de quien aporta el material, la forma en que se accedió a su contenido, la naturaleza institucional del equipo que la soporta, o la certeza de que el mensaje fue realmente enviado por quien se dice.

En ese orden de consideraciones, podemos concluir que el carácter institucional de un equipo o del sistema empleado no basta por sí solo para excluir toda expectativa de privacidad, como lo demuestran los dictámenes Nos 74.351, de 2011, y 10.352, de 2019.

A su vez, cuando el material es aportado por los intervinientes de la conversación, la expectativa no resulta oponible cuando la presenta como prueba en un proceso disciplinario, tal como lo indica el dictamen E288163, de 2022.

Una tercera hipótesis que aborda la jurisprudencia administrativa analizada dice relación con la insuficiente acreditación de la autoría de los mensajes, lo que se distingue con claridad en los dictámenes Nos 13.520, de 2017, y 1.127, de 2021.

La referida fragmentación de criterios, aunque no es lo ideal, sí permite distinguir una línea jurisprudencial, que, ordenada de la forma anteriormente expuesta, puede otorgar cierto grado de predictibilidad a los operadores del derecho que necesiten vislumbrar cómo la Entidad Contralora ha resuelto casos similares.

Finalmente, ante la necesidad de argumentar un caso no resuelto, ya sea como fiscal o defensor, insistimos en la aplicación del test de Katz, en su forma originalmente concebida por el Juez Harlan, o por el contrario, atender a la crítica del profesor Kerr para, por ejemplo, impugnar un análisis que formule dicha prueba sin completar sus dos pasos.

⁸ En este pronunciamiento se analiza no solo en el soporte físico institucional del programa, sino que también el control sobre la plataforma, que, aunque privada, es objeto de una revisión por parte de personal del municipio bajo el contexto de una revisión general de computadores institucionales para detectar mal uso de éstos.

Bibliografía

ESCOBAR VEAS, JAVIER (2023). «Redes sociales y expectativa legítima de privacidad en la jurisprudencia de la Corte Suprema chilena». *Revista Chilena de Derecho y Tecnología*, 12, pp. 1-27. DOI: 10.5354/0719-2584.2023.69893.

GARCÍA MESCUA, DANIEL (2018). *Aportación de mensajes de WhatsApp a los procesos judiciales: tratamiento procesal*. Granada: Comares.

ISENSEE RIMASSA, CARLOS (2018). *Prueba y medidas cautelares en el derecho administrativo sancionador, penal y civil*. Santiago: Librotecnia.

KERR, ORIN S. (2015). «Katz Has Only One Step: *The Irrelevance of Subjective Expectations*». *The University of Chicago Law Review*, 82, pp. 113-168.

ROCO LEHYT, CECILIA (2022). *La prueba de las comunicaciones electrónicas en los procedimientos administrativos disciplinarios regidos por la Ley N° 18.834*. Tesis de magíster, Universidad de Chile.

Jurisprudencia

Contraloría General de la República, dictamen N° 74.351, de 2011.

Contraloría General de la República, dictamen N° 44.894, de 2014.

Contraloría General de la República, dictamen N° 35.523, de 2016.

Contraloría General de la República, dictamen N° 13.520, de 2017.

Contraloría General de la República, dictamen N° 36.110, de 2017.

Contraloría General de la República, dictamen N° 13.606, de 2018.

Contraloría General de la República, dictamen N° 10.352, de 2019.

Contraloría General de la República, dictamen N° 7.849, de 2020.

Contraloría General de la República, dictamen N° 1.127, de 2021.

Contraloría General de la República, dictamen E155404, de 2021.

Contraloría General de la República, dictamen E288163, de 2022.

Corte de Apelaciones de Copiapó, 26 de enero de 2025, rol N° 416-2024.

Katz v. United States, 389 U.S. 347 (1967), Supreme Court of the United States.