Universidad de Chile Facultad de Derecho Departamento de Derecho Procesal

Taller “La prueba civil y los modernos medios representativos y la Firma electrónica”

Profesora Lorena Donoso Abarca

GEOLOCALIZACIÓN DE TELÉFONOS CELULARES A PARTIR DE LOS DATOS DE TRÁFICO:

MEDIO DE PRUEBA EN SEDE PENAL

Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

JULIÁN RODRÍGUEZ SAAVEDRA

Autor

LORENA DONOSO ABARCA

Profesora Guía

Santiago de Chile

2022

Agradecimientos

Quisiera agradecer a la profesora Lorena Donoso Abarca por su orientación e inspiración en la realización de este trabajo; pero, sobre todo, por su infinita paciencia.

Asimismo, quisiera agradecer al profesor Eduardo Costoya, que sin su participación habría sido imposible iniciar este trabajo. Gracias por abrir las puertas de su casa, por aquellos cafés recién granulados y las tertulias frente al piano.

Índice

Índice de ilustraciones

ABREVIATURAS Y ACRÓNIMOS

BTS	Del inglés Base Transceiver Station. Estaciones base
CA	Corte de Apelaciones
CS	Corte Suprema
CADH	Convención Americana sobre Derechos del Hombre
CE	Consejo Europeo
CDN	Convención sobre los Derechos del Niño
CDR	Call Detail Recorder
CGR	Contraloría General de la República
CIDH	Corte Interamericana de Derechos Humanos
CPP	Código Procesal Penal
CPR	Constitución Política de la República de Chile
DADDH	Declaración Americana de los Derechos y Deberes del Hombre
DS	Decreto Supremo
DUDH	Declaración Universal de Derechos Humanos
HLR	Home Location Register
ICDT.	Instituto Chileno de Derecho y Tecnologías
IMEI	International Mobile Equipment Identity
LECr	Ley de Enjuiciamiento Criminal Española
OCDE	Organización para la Cooperación y el Desarrollo Económicos
ONU	Organización de Naciones Unidas
PIDCP	Pacto Internacional de Derechos Civiles y Políticos

RAE	Real Academia Española
RUC	Rol Único de la Causa
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
UE	Unión Europea
UIT	Unión Internacional de las Telecomunicaciones

Resumen

A la luz del desarrollo tecnológico actual y la necesidad de ingeniar nuevas maneras de acreditar la comisión de delitos y la participación de los sospechosos en estos, el siguiente trabajo tiene por finalidad analizar jurídicamente una metodología que permite utilizar el sistema de geolocalización de los teléfonos celulares como medio de prueba para acreditar la ubicación de un sospechoso dentro de un radio o intersección acotados cercanos al sitio del suceso; constituyendo un sólido indicio de su participación en el mismo.

El método analizado, propone utilizar la información que las antenas y celdas de las compañías de telecomunicación recopilan de manera automática con posterioridad a la realización o recepción de llamadas, asociada a los datos de los terminales de usuarios de los sospechosos (y eventualmente las víctimas), en base a la metodología propuesta por el Colegio de Ingenieros de Chile.

El trabajo consta de cuatro secciones. La primera está dedicada a la explicación técnica del método con que se llega a la geolocalización del teléfono celular, incluyendo conceptos básicos de telecomunicaciones y una reseña histórica, prosiguiendo con el desarrollo de la técnica en sí.

La segunda sección está destinada a analizar la normativa sustantiva y procesal dentro de la que se enmarca este tipo de medida investigativa, partiendo por regulación del debido proceso; la necesidad de solicitar autorización judicial; la manera de presentarla en juicio; aspectos relativos a la prueba, tales como la valoración y el estándar probatorio.

La tercera parte, se refiere a la interacción de la geolocalización con los Derechos Fundamentales consagrados en Instrumentos Internacionales y en la Constitución Política.

Finalmente, la sección cuarta está dedicada a un análisis del tratamiento jurídico que se da en derecho comparado a esta medida investigativa, particularmente en España, incluyendo un breve análisis desde la perspectiva de los derechos fundamentales con que colisiona. Incluimos también el análisis de una sentencia del Tribunal Supremo Español en que se refiere a la acreditación de los hechos y la participación mediante indicios o hechos base. También se estudia el tratamiento jurídico en Perú, país de nuestro entorno en que encontramos algunas referencias útiles a nuestras reflexiones.

Introducción

> Al cuarto día de haber cometido el asesinato se presentó, inopinadamente, en mi casa un grupo de agentes de Policía, y procedió de nuevo a una rigurosa inspección. Confiado en lo impenetrable de aquel escondite, no experimenté turbación alguna.
>
> El gato negro. Edgar Allan Poe[1]

Gracias al exponencial progreso de las tecnologías, la impunidad criminal está cada día más cerca de ser vencida.

En Chile, desde al menos dos décadas, las telecomunicaciones han pasado a ser fundamentales dentro del vivir de toda persona, que se ha beneficiado del poder e inmediatez que los aparatos proporcionan.

A partir de los años 2000, la masificación de los teléfonos celulares vino a reemplazar al teléfono fijo, permitiendo a las personas mantenerse conectados aun cuando se encuentre en lugares remotos, lo que hasta entonces no era posible con la telefonía fija. Asimismo, los mensajes de texto reemplazaron algunas funciones que cumplía masivamente el fax (que, a su vez, en los años noventa había reemplazado en parte a los correos comunes y corrientes) y menos intensamente el correo electrónico.

En los años previos al inicio de la segunda década de este siglo, se consagró en nuestro país la utilización del internet; que trajo consigo la masificación de los correos electrónicos en el aspecto más formal, y plataformas como Messenger y luego Facebook para comunicaciones coloquiales.

Finalmente, aproximadamente desde el año 2012 a esta parte, el fenómeno de los teléfonos inteligentes ha irrumpido, provocando efectos mayores que cualquiera de las innovaciones

[1] ALLAN POE, EDGAR (2010) *Narraciones Extraordinarias*. Santiago de Chile: Zig-zag, p.16.

anteriores, puesto que abrió un universo virtualmente infinito de posibilidades de todo orden. Aquí destaca la utilización de WhatsApp, que trajo consigo la posibilidad de comunicarse a través de multimedia, esto es, mensajes de texto, imágenes, videos, audios, emojis, GIF's y los últimamente famosos "stickers". Incluso es posible el envío de archivos de variados tipos, tales como documentos, videos, fotografías; lo que viene a significar una alternativa al correo electrónico; más aún con la posibilidad de conectarse a WhatsApp desde cualquier computador a través de su plataforma "WhatsApp Web".

Si bien las generaciones más jóvenes han reemplazado las llamadas telefónicas por la mensajería electrónica instantánea, aquéllas no han perdido relevancia en el mundo adulto, toda vez que supone un inmediatez y conexión humana incomparable.

Sin embargo, la comunicación telefónica no siempre es usada con propósitos legítimos, sino que se usan para efectuar estafas o concertarse para delinquir de variadas maneras.

Ahora bien, aunque parezca contradictorio, el uso de las telecomunicaciones por parte de los delincuentes trae consigo una ventaja importante, que consiste en la posibilidad de proveer de diversas evidencias que permiten acreditar la comisión de un delito y la participación de los sospechosos en este. Una de las herramientas que proporciona es la geolocalización o georreferenciación como fuente de prueba, a la cual nos referiremos en nuestra investigación.

Si bien no son pocos los casos en que la fiscalía solicita que se entregue información sobre tráfico de llamadas de una determinada zona para investigar la comisión de un delito[2], hemos advertido, que se enfrentan dificultades por la falta de especificidad de la normativa actual.

A mediados de la primera década de los años dos mil, la legislación procuró al Ministerio Público y a las policías de la interceptación de las comunicaciones, regulada en Código Procesal Penal y a través de un Reglamento. Lo que ha tenido especial relevancia en la prevención de delitos. No obstante, junto con las nuevas medidas de investigación, surgen nuevas posibilidades de que estas afecten derechos fundamentales reconocidos por la Constitución y los Instrumentos Internacionales suscritos y ratificados por Chile; primero la protección de la vida privada y el secreto de las comunicaciones; y, desde hace algunos años, la protección de los datos personales,

[2] 24 HORAS (2018) Analizarán tráfico de llamadas de sector donde murió Camilo Catrillanca [en línea] <https://www.24horas.cl/nacional/analizaran-trafico-de-llamadas-de-sector-donde-murio-camilo-catrillanca--2883921> [consultado el 20 de octubre de 2020].

derecho que se consagró el año 2018 en la Constitución como una respuesta a la masificación del tratamiento de datos producto del avance tecnológico[3].

Por otro lado, como veremos más adelante, la legislación procesal penal no cuenta con una regulación detallada de medidas investigativas similares a la interceptación, pero de notables características propias. De manera que actualmente, cuando se pretende recabar información de las empresas de telecomunicaciones, se hace rigiéndose por la normativa dedicada a la interceptación, la que si bien supone una mucho mayor injerencia y vulneración de derechos fundamentales, no es la opción más idónea si consideramos que al afectarse garantías fundamentales las normas deben ser interpretadas de manera restrictiva y en este casos se estaría haciendo una aplicación extensiva a hipótesis no consideradas por el legislador. Veremos que en derecho comparado se ha regulado de manera pormenorizada esta materia. Es la situación de año 2020, trajo consigo un aumento sustancial en la utilización de las telecomunicaciones, sea para trabajar o bien para cualquier tipo de entretenimiento social, con la finalidad de evitar el contacto físico entre las personas. La delincuencia también aprovechó las tecnologías para llevar adelante su actividad y, los teléfonos celulares fueron una de las herramientas más usadas para ello.

Para salvarlas, en nuestro trabajo recurrimos a la prueba indiciaria, aprovechando las posibilidades que ofrecen las tecnologías de la información y las comunicaciones. Se trata de un método que aprovecha la forma de funcionamiento de la telecomunicación celular, los datos que entregan las empresas operadoras de telecomunicación, en combinación con técnicas provenientes de la matemática de probabilidades conjuntas, entre otras, con el fin de geolocalizar la ubicación de determinadas personas en una fecha y hora precisa, para demostrar así que tuvo participación en el delito.

En la exposición de resultados de nuestra investigación, damos cuenta de la manera en que se regula actualmente la entrega de información por parte de las empresas operadoras a las

[3] Antes de la entrada en vigor de esta norma, los datos personales estaban protegidos a nivel legal por la Ley 19.628, que data de 1999, y que actualmente no cumple con los estándares y necesidades de un mundo globalizado en que predominan las telecomunicaciones de manera tan masiva. De hecho, a esta fecha se encuentra en tramitación el proyecto de ley que viene actualizar dicha normativa legal, que consagra nuevos principios y una detallada regulación.

fiscalías, tanto en Chile como en el Derecho Comparado, con el fin de que las fiscalías del país puedan orientarse respecto a la información que resulta útil de solicitarles a los operadores.

Si bien, a mediados de la primera década de los años dos mil, la legislación reguló en el Código Procesal Penal la interceptación de las telecomunicaciones por el Ministerio Público, lo cual fue desarrollado y a través de un Reglamento, lo que ha tenido especial relevancia en la prevención de delitos, junto con las nuevas medidas de investigación, surgen nuevas posibilidades de que estas afecten derechos fundamentales reconocidos por la Constitución y los Instrumentos Internacionales suscritos y ratificados por Chile; primero la protección de la vida privada y el secreto de las comunicaciones; y, desde hace algunos años, la protección de los datos personales, derecho que se consagró el año 2018 en la Constitución como una respuesta a la masificación del tratamiento de datos producto del avance tecnológico[4].

Adicionalmente y como veremos más adelante, la legislación procesal penal no cuenta con una regulación detallada de otras medidas investigativas similares a la interceptación, pero de notables características propias. De manera que actualmente, cuando se pretende recabar información de las empresas de telecomunicaciones, se hace rigiéndose por la normativa dedicada a la interceptación, la que supone una mucho mayor injerencia y vulneración de derechos fundamentales, a diferencia de otras legislaciones en que sí se ha regulado de manera pormenorizada, como es el caso de España, que tiene para las distintas medidas investigativas que vulneran derechos fundamentales.

La relevancia de la investigación dice relación con la masividad de los servicios de telefonía para las comunicaciones de las personas, en todos los ámbitos que ya se avistaba antes de la crisis pandémica provocada por la proliferación del COVID-19. Luego a partir del año 2020, se ha visualizado un aumento sustancial en la utilización de las telecomunicaciones, sea para trabajar, estudiar o bien para cualquier tipo de entretenimiento social, con la finalidad de evitar el contacto físico entre las personas. La delincuencia también aprovechó las tecnologías para

[4] Con anterioridad a esta norma constitucional, los datos personales estaban protegidos a nivel legal por la Ley 19.628, que data de 1999, ley que actualmente no cumple con los estándares y necesidades de un mundo globalizado en que predominan las telecomunicaciones de manera tan masiva. De hecho, a esta fecha se encuentra en tramitación el proyecto de ley que viene actualizar dicha a ley, que consagra nuevos principios y una detallada regulación.

llevar adelante su actividad y, los teléfonos celulares fueron una de las herramientas más usadas para ello.

Siendo así, resulta evidente la necesidad de contar con normas jurídicas que regulen las diversas acciones de investigación y prueba asociadas a los registros de las telecomunicaciones, cuando son empleadas con ocasión de la comisión de un delito o en aquellos casos que las comunicaciones contengan información relevante a los efectos de esclarecer los hechos de un proceso.

Adicionalmente, advertimos que, tratándose de un tema técnico, es necesario analizar el funcionamiento de las redes y las técnicas empleadas para el análisis de las comunicaciones, pues estos conocimientos son necesarios para que los operadores jurídicos puedan aproximarse al objeto de nuestra investigación.

El objetivo general de nuestro trabajo es **fijar las bases metodológicas de la recogida, conservación y presentación en juicio, como prueba de la participación de un sujeto en un delito, de los datos de georreferenciación de dispositivos móviles.** El **método utilizado** es la investigación documental, mediante la **técnica** de fichaje, esto es, investigación documental bibliográfica. El trabajo constará de diversas secciones, cada una destinada a cumplir un objetivo específico:

El primer objetivo específico es describir y explicar el informe de peritos de la Comisión de Telecomunicaciones del Colegio de Ingenieros, presidida por el profesor **Eduardo Costoya**, quien amablemente contribuyó de manera activa en la realización de la presente investigación, proporcionando los conocimientos técnicos que sobrepasan lo meramente jurídico. Esta primera parte se divide en dos subsecciones; la primera, que se refiere someramente a los conceptos necesarios para comprender la técnica de localización, tales son las telecomunicaciones, radiofrecuencias, celda, antenas de cobertura omnidireccional y direccional, entre otras. La segunda subsección se refiere a la técnica de georreferenciación como tal, incluyendo la totalidad del proceso que se debe seguir y la información que se debe requerir de las operadoras para llevarlo a cabo exitosamente.

En segundo lugar se busca realizar un análisis jurídico, tanto de las normas dentro de las que se circunscribe este proceso de georreferenciación, como de las potenciales limitaciones frente a garantías constitucionales, sobre todo en lo respectivo a la entrega de información por parte de

las empresas operadoras de telecomunicaciones. Asimismo, se analizan los principales aspectos relativos a la prueba de estos indicios y sus efectos en el proceso.

En tercer lugar, se realiza un análisis de derecho comparado, para lo cual se esboza la regulación jurídica que esta medida de investigativa tiene en España, incluyendo su colisión con los derechos fundamentales. Incluyendo el análisis de una sentencia del Tribunal Supremo Español, que se refiere a la acreditación de los hechos y participación a partir de indicios o hechos base. Asimismo, se incluye el tratamiento jurídico del Perú.

Adicionalmente, se analiza la regulación jurídica que este tipo de medidas investigativas en España, incluyendo su colisión con los derechos fundamentales. Incluyendo el análisis de una sentencia del Tribunal Supremo Español, que se refiere a la acreditación de los hechos y participación a partir de indicios o hechos base. Asimismo, se incluye el tratamiento jurídico del Perú.

Capítulo I. Técnica de geolocalización.

Este capítulo nos permitirá entender de qué manera pueden utilizarse los datos de tráfico de una llamada telefónica para localizar un teléfono celular en una fecha y hora determinadas, de forma tal que dé cuenta de la presencia de un sospechoso en el sitio del suceso.

El sistema que aquí se describe fue desarrollado por el profesor, ingeniero eléctrico, presidente de la Comisión de Telecomunicaciones del Colegio de Ingenieros de Chile A.G., Eduardo Costoya.

Este método técnico se basa, principalmente, en:

1. Propagación de ondas
2. Tecnología de telecomunicaciones mediante celular
3. Principios matemáticos de probabilidades conjuntas

Para entenderlo mejor, es necesario entregar una breve introducción de conceptos básicos, que nos permitan comprender el funcionamiento de las redes de telecomunicaciones.

1. Telefonía Celular. Principios básicos y georreferenciación de coberturas.

a. Comunicaciones.

Primero que todo debemos hacernos cargo de los tipos de comunicación más comunes, a saber, las comunicaciones alámbricas y las comunicaciones inalámbricas.

Las **comunicaciones alámbricas** se caracterizan por transmitir información a través de un medio físico, "codificando información en forma de señales eléctricas, a través de medios conductores de la electricidad, como los cables de cobre".[5] En resumen, se puede mencionar como primer sistema de comunicación alámbrica el telégrafo, originado a finales del siglo XIX.

[5] RLOPEZ33 Blog (s/f) *Comunicaciones alámbricas* [En línea] <https://sites.google.com/site/tecnorlopez39/home/tema-7-comunicaciones/2-comunicacion-alambrica> [Visto en línea 12/10/2020].

En efecto, el teléfono fue presentado en la exposición del centenario de la independencia de Estados Unidos, realizada en Filadelfia, en la que obtuvo el máximo galardón, imponiéndose sobre los otros avances científicos que en ella se expusieron. Junto con ello, en esta misma exposición realiza su primera venta, 100 teléfonos para la Corte del Emperador de Brasil, don Pedro I.[6] No obstante, su deslucida entrada al mercado de las comunicaciones, provocada en parte importante por las resistencias que impuso la empresa de telégrafos de la época al ver amenazados sus intereses (cosa no poco frecuente hoy en día), la penetración de este aparato no se hizo esperar.

En 1921 había próximamente 13 millones de teléfonos conectados a las líneas de la *American Telephone and Telegraph Company*, y medio millón más sin considerar la propiedad; es decir, uno por cada ocho personas. Sus circuitos contenían 40.000.000 de kilómetros de hilo y sus empleados pasaban de 231.000. El promedio de los despachos transmitidos diariamente en esta red excedía los 33.000.000.[7]

Desde entonces hubo distintos sistemas hasta llegar al más reconocido hoy, cuál es el teléfono de red fija.

Por otra parte, tenemos la **comunicación inalámbrica**, que es definida como una "comunicación que se realiza entre dos dispositivos que no están conectados por un cable físico, sino que utilizan el espectro electromagnético".[8] También se han definido como "redes que utilizan ondas de radio para conectar los dispositivos, sin necesidad de utilizar cables de ningún tipo".[9]

---

[6] DE LA PEÑA, JOSÉ. *Historia de las Telecomunicaciones*. Ariel Derecho, 2003, pág. 33.

[7] SAPIENSMAN (s/f) *Historia de la comunicación por alambres: inicios del telégrafo y el teléfono*, publicación electrónica, disponible on-line: http://www.sapiensman.com/old_wires/telegrafo_y_telefono3.htm [Visto en línea 11/10/2021].

[8] REAL ACADEMIA DE INGENIERÍA DE ESPAÑA (s/f) *Diccionario español de ingeniería: definición de comunicación inalámbrica*. [en línea] http://diccionario.raing.es/es/lema/comunicaci%C3%B3n-inal%C3%A1mbrica [Visto en línea 17/11/2021].

[9] SALAZAR, JORDI (2016)*Redes inalámbricas*, České vysoké učení technické v Praze Fakulta elektrotechnická, (only electronic form). TechPedia. European Virtual Learning Platform for Electrical and Information Engineering. http:///www.techpedia.eu. Disponible en línea en https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf [Visto en línea 11/10/2021].

El desarrollo de esta tecnología surge a partir del trabajo de Michael Faraday sobre **inducción electromagnética**, del año 1850.

Dos años más tarde, Oliver Lodge (1851-1940), también inglés, basándose en el trabajo de Crookes, construye el primer sistema de comunicación inalámbrica que incluía un circuito sintonizador, a través del cual demostró la recepción de una señal a través de una distancia aproximada de 100 m, enviando señales de una a otra orilla a través del Canal de Bristol.

Casi veinte años más tarde, en 1968, James C. Maxwell establece las **bases matemáticas de las ondas electromagnéticas**.

Posteriormente, Marconi, en 1896 obtiene del gobierno inglés la primera patente, en ese entonces de telegrafía inalámbrica, en 1898 transmite de un lado al otro del canal de la mancha y en 1901 logra el mayor proyecto de la época, comunicar Cornwall, en Gran Bretaña con San Juan de Terranova, Canadá, toda una hazaña para la época.

La idea de aplicar las ondas hertzianas a la telegrafía sin hilos se atribuye al inglés William CROOKES (1832-1919), quien en 1892 publicó un trabajo en la revista inglesa Fortnightly Review, en el que proponía las bases para utilizar ondas electromagnéticas como medio para transmitir señales telegráficas a través del aire, sin hilos o inalámbrica[10] y adaptó el manipulador y el receptor de Morse para ser empleado en esta aplicación.

Finalmente, Alexander S. Popov en 1895 construyó y probó **la primera antena.** [11]

Tal era el impacto político y social del telégrafo que los Estados se vieron en la necesidad de propiciar acuerdos internacionales de interconexión, proceso que finalmente desencadenó que el 17 de mayo de 1865, tras dos meses y medio de arduas negociaciones, 20 estados de Europa firmaron en París el primer Convenio Telegráfico Internacional y crearon la Unión Telegráfica Internacional, con objeto de facilitar posibles modificaciones posteriores a este acuerdo inicial.

[10] BRAUN, ELIÉCER (1992) *Electromagnetismo, de la ciencia a la tecnología*. Capítulo XVIII "Inicio de las comunicaciones inalámbricas. Marconi". Ed. Fondo de Cultura Económica. Primera Edición, México. Disponible on-line en http://omega.ilce.edu.mx:3000/sites/ciencia/volumen_3/ciencia3/112/htm/electr.htm. [Visto en línea 11/10/2021].

[11] Ibid.

Hoy, unos 135 años después, los motivos que llevaron a la creación de la UIT siguen siendo de actualidad y los objetivos fundamentales de la organización son básicamente los mismos.[12]

Tal fue la importancia de la telegrafía que rápidamente se instó la necesidad de su regulación y fue así como se convocó la primera convención internacional destinada a estudiar el tema de la regulación de la telegrafía, la que se celebró en Berlín en 1906 en el que se firmó el primer Convenio Internacional de Radiotelegrafía, cuyo anexo contiene las primeras normas sobre telegrafía sin hilos.

Como ejemplos más significativos de sistemas que ocupan este tipo de comunicación tenemos la radiodifusión, tanto AM como FM, la televisión analógica, televisión digital, televisión satelital, **telefonía celular**, redes de datos y la telefonía satelital.

b. Ondas.

Una onda es una "[p]erturbación que se propaga a una velocidad determinada en un medio material de forma que, en cada punto del medio, la magnitud que sirve para medir la perturbación es una función del tiempo, mientras que, en cualquier instante, la misma magnitud, en un punto, es función de las coordenadas de este punto"[13]. Además, se trata de "un movimiento periódico que se propaga en un medio físico o en el vacío".[14]

Se pueden distinguir distintas ondas en la naturaleza, tales como la onda en el agua, onda sísmica, onda sonora**, onda electromagnética**. El diccionario de la Real Academia Española de la Lengua define estas última como "[f]orma de propagarse a través del espacio los campos eléctricos y magnéticos producidos por las cargas eléctricas en movimiento. Para las ondas

[12] UNIÓN INTERNACIONAL DE LAS TELECOMUNICACIONES (2015*) Paris 1865: Nacimiento de la Unión. Documento publicado con ocasión del 159° aniversario de la Creación de la Unión Internacional de las Telecomunicacione*s, Publicación electrónica. Disponible on-line en https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/12.36.72.es.300.pdf [Visto en línea 20/10/2021].

[13] REAL ACADEMIA DE INGENIERÍA DE ESPAÑA (s/f) *Diccionario español de ingeniería: definición de onda* op. cit.

[14] REAL ACADEMIA ESPAÑOLA (s/f) *Diccionario de la lengua española: definición de onda* [en línea] https://dle.rae.es/onda?m=form [Visto en Línea 17/11/2021].

comprendidas entre diferentes intervalos de frecuencia se emplean denominaciones especiales, como ondas radioeléctricas, microondas, ondas luminosas, rayos X, rayos gamma, etc".[15]

Estas ondas "se generan por la vibración de electrones u otras partículas con carga eléctrica. La energía producida por esta vibración viaja en forma de ondas electromagnéticas".[16] Entre ellas tenemos las ondas de radio televisión y telefonía, que pueden generarse por corrientes variables en distintos tipos de **antenas.**[17]

En Chile el Plan General de Uso del Espectro Radioeléctrico se refiere a las **ondas radioeléctricas u ondas hertzianas**, definiéndolas como "ondas electromagnéticas, cuya frecuencia se fija convencionalmente por debajo de 3000 GHz, que se propagan por el espacio sin guía artificial".[18]

En derecho comparado, el Reglamento Telecomunicaciones de México, define Ondas Radioeléctricas en los siguientes términos: "Son ondas electromagnéticas, cuyas frecuencias se fijan convencionalmente por debajo de 3000 GHz, que se propagan por el espacio sin guía artificial"[19]

Telecomunicación.

Las telecomunicaciones son "todas aquellas formas de comunicación entre personas donde existe distancia geográfica, por medios radiofónicos, electrónicos o telemáticos".[20]

---

[15] Ibid.

[16] SCENIH (2008) *Scientific Comittee on Emerging and Newly Identified Health Risks*. *Light Sensivity*. Adopted an 26TH Plenary on 23.09.2008. Disponible en línea en https://ec.europa.eu/health/ph_risk/committees/04_scenihr/docs/scenihr_o_019.pdf [Visto en línea 15/11/2021].

[17]MELIÁ MIRALLES, JOAQUÍN (1991) *Fundamentos físicos de la teledetección: leyes y principios básicos;* En *la teledetección en el seguimiento de los recursos naturales*, Universidad de Valencia. p.51 [en línea] https://books.google.cl/books?id=t8ZLSpM20m8C&pg=PA51&redir_esc=y#v=onepage&q&f=false [Visto en línea 17/11/2021].

[18] Art. 1, Decreto N° 127, que aprueba plan general de uso del espectro radioeléctrico. Términos y Definiciones. Sección I. Términos generales, 1.4.

[19] Reglamento de Telecomunicaciones. Diario Oficial de la Federación del 29 de octubre de 1990, disponible en línea en http://www.sct.gob.mx/JURE/doc/regl-telecomunicaciones.pdf [consulta: 06.01.2022].

[20] LARA, JUAN CARLOS; PINCHEIRA; VERA (s.f.) *La privacidad en el sistema legal chileno*. ONG Derechos Digitales. P. 70 Disponible en línea https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf [Visto en línea 11/11/2021].

La ley 18.168, General de Telecomunicaciones, siguiendo al Reglamento Internacional de Comunicaciones de la UIT,[21] define telecomunicación, en su artículo 1, como "toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos e informaciones de cualquier naturaleza, por línea física, radioelectricidad, medios ópticos u otros sistemas electromagnéticos".

Conforme al artículo 19 N° 5 de la Constitución Política de la República, en Chile se protege el secreto de toda comunicación privada. Consecuentemente con lo anterior, los prestadores de servicios de telecomunicaciones tienen un deber de reserva sobre las comunicaciones. A su vez, el Decreto N° 18, de 09 de enero de 2014, que "*aprueba el Reglamento de Servicios de Telecomunicaciones que indica*", los prestadores de servicios de telecomunicaciones tienen un deber de reserva sobre el contenido de las comunicaciones, cualquiera sea el servicio específico que se emplee por los usuarios.

c. Antena.

Una antena es un "[d]ispositivo metálico capaz de emitir ondas electromagnéticas al medio que le rodea cuando se le aplica una señal eléctrica y generar una señal eléctrica cuando está expuesto a una onda electromagnética y viceversa".[22] En términos simples una antena transmisora transforma energía eléctrica en ondas electromagnéticas, y una receptora realiza la función inversa.[23] Es un mecanismo que permite comunicar datos a través de un medio no guiado como es el caso de las comunicaciones móviles, de telefonía, radiocomunicación, radio de punto a punto -policías, bomberos-.

[21] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (1989) *Reglamento de telecomunicaciones internacionales* [En línea] https://www.itu.int/dms_pub/itu-t/oth/3F/01/T3F010000010001PDFS.pdf. [Visto en línea 15/11/2021].

[22] REAL ACADEMIA DE INGENIERÍA DE ESPAÑA (s/f) *Diccionario español de ingeniería: definición de antena* op.cit.

[23] Ibid.

Por su parte, el prestigioso IEEE (Institute of electrical and electronics Engineers) define una antena como "aquella parte de un sistema transmisor o receptor diseñada especialmente para radiar o recibir ondas electromagnéticas"[24].

A propósito de las antenas, tenemos la BTS, cuyas siglas en inglés significan *Base Transceiver Station*, conocido en español como **estación base**.

Estación base es el "[c]onjunto de uno o más emisores o receptores de radio, o una combinación de emisores y de receptores incluyendo los equipos asociados, que permite, en un emplazamiento dado, asegurar un servicio de radiocomunicación o de radioastronomía".[25] Básicamente, es una "[i]nstalación destinada a proporcionar acceso al sistema de telecomunicaciones por medio de ondas de radio".[26]

Una estación base, por lo general, va a contener varias antenas, normalmente sectoriales, es decir, que cubren determinado sector geográfico.

La información está transmitida mediante un código, a saber, la modulación, la cual es definida como "[p]roceso por el que una magnitud característica de una oscilación u onda, sigue las variaciones de una señal o de otra oscilación u onda". A ello agrega que "[l]a modulación puede ser intencional o no intencional".[27]

En efecto, la legislación de cada país se encarga de asignar tramos del espectro de frecuencias a distintas empresas operadoras de telecomunicaciones, las cuales a través de la modulación obtienen que se pueda transmitir mayor cantidad de información sin sobrepasarse de su respectivo tramo asignado del espectro. La UIT, en su manual sobre la gestión nacional del

---

[24] IEEE (1983*) Standard Definitions of Terms for Antennas, Std 145-1983*, Revision of ANSI/IEEE Std 145-1973 [en línea] <https://ieeexplore.ieee.org/document/30651> [Visto en línea 15/11/2021].

[25] REAL ACADEMIA DE INGENIERÍA DE ESPAÑA (s/f) *Diccionario español de ingeniería: op. Cit.*

[26] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (2021) T*raducción libre del texto: "Installation intended to provide access to the telecommunication system by means of radio waves." ITU-T, K.56 (05/2021), Series K: Protection against interference. Protection of radio base stations against lightning discharches*". Disponible en línea en https://www.itu.int/rec/T-REC-K.56-202105-I/es, [Visto en línea 15/11/2021].

[27] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (1993) *UTI-R V.662-2. Recomendación UIT-R V.662-2 "Términos y definiciones (1986-1990-1993*). [En línea] https://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.662-2-199304-S!!PDF-S.pdf [Visto en línea 15/11/2021].

espectro radioeléctrico, entrega los lineamientos generales a las que deben ceñirse los países[28]. En el caso de Chile el plan general de uso del espectro radioeléctrico vigente fue aprobado por Decreto N° 127 del Ministerio de Transportes y Telecomunicaciones, Subsecretaría de Telecomunicaciones, de 2006, actualizado el 30 de julio de 2016.

d. Antena sectorial.

Es una especie de antena de microondas direccional que tiene un patrón de radiación en forma de sector circular, que, en su sentido geométrico se refiere a una circunferencia medida en grados de arco. Un sector es la porción de círculo limitada por dos radios. Se encuentran típicamente en diseños de 60°, 90° y 120°.[29]

Este tipo de antena presenta características propias de antenas direccionales como omnidireccionales. Las direccionales tienen un haz estrecho, pero de largo alcance; las segundas tienen un haz amplio, pero de corto alcance. Así, las antenas sectoriales mezcla de ambas, emiten un haz de amplitud intermedia y tienen un alcance también intermedio.

En una instalación se encuentran normalmente tres antenas sectoriales de 120° o bien cuatro antenas sectoriales de 80°, teniendo la finalidad de cubrir los 360°.

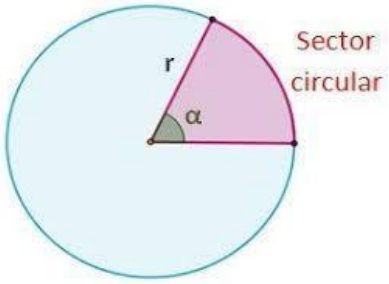

ILUSTRACIÓN 1

En telecomunicaciones cada sector circular es denominado y considerado como **azimut** (o acimut), que, como puede verse en la imagen a continuación, utiliza el Norte como guía:

[28] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (2015) *Manual sobre la gestión nacional del espectro*. Disponible en línea en https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-21-2015-PDF-S.pdf. [Visto en línea 15/11/2021].

[29] MENDOZA, E.; PUERTAS, JOSÉ; MONTERO, JOSÉ (2017) *Antenas sectoriales* [en línea] <https://es.slideshare.net/ErnestoMendoza10/antenas-sectoriales> [Visto en línea 15/11/2021].

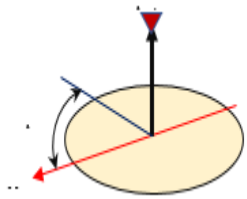

ILUSTRACIÓN 2

En la fotografía satelital a continuación se puede apreciar el área geográfica que cubre un acimut:

ILUSTRACIÓN 3

e. Comunicación celular (la celda).

La telefonía celular o telefonía móvil se define como el "sistema telefónico en el que la conexión entre el aparato portátil y la central se realiza mediante ondas hertzianas".[30]

Se llama celda a una pequeña área geográfica de carácter hexagonal a que una antena o estación base tiene alcance y que es necesaria para que exista una comunicación efectiva para el usuario móvil.[31]

[30] REAL ACADEMIA ESPAÑOLA (s/f) *Diccionario de la lengua española: definición de telefonía celular* [en línea] https://dle.rae.es/telefon%C3%ADa. [Visto en Línea 15/11/2021].

[31] ORANGE. (s/f) *¿cómo funciona una red móvil?* [en línea] <https://radio-waves.orange.com/es/como-funciona-una-red-movil/> [Visto en línea 17/03/2020].

“Cada estación base cubre una celda, por consiguiente, un conjunto de estaciones bases conforman las llamadas redes de celdas o redes celulares, que proporcionan cobertura de radio en áreas geográficas más extensas. Por lo tanto, el equipo de usuario (UE), como los teléfonos móviles, puede comunicarse incluso si el equipo se mueve a través de las células durante la transmisión”.[32]

El tamaño de las celdas se diferencia principalmente en cuanto si son en zonas urbanas o rurales y una proyección de la demanda de conexión, que realiza el proveedor de que se trate. En el primer caso, al haber alta densidad de población las celdas tienden a ser numerosas y pequeñas. En cambio, en zonas rurales las celdas son de mayor tamaño y por tanto de mayor cobertura. En estas últimas es común que se utilicen antenas omnidireccionales.

En resumen, el procedimiento es el siguiente:

“En su operación, el teléfono móvil establece comunicación con una estación base y, a medida que se traslada, los sistemas computacionales que administran la red van transmitiendo la llamada a la siguiente estación base de forma transparente para el usuario. Por eso se dice que las estaciones base forman una red de celdas, sirviendo cada estación base a los equipos móviles que se encuentran en su celda”.[33]

Por lo general, en zonas residenciales en que no hay construcciones en altura, las celdas se encuentran a una distancia de 1.5 a 2 km entre ellas. En zonas más congestionadas, como por ejemplo Santiago Centro, la distancia se reduce a 500 a 600 metros. En las zonas urbanas, con alta densidad de población y un número importante de comunicaciones, las celdas tienden a ser numerosas y pequeñas (a cientos o incluso a sólo unas decenas de metros de distancia). En las zonas rurales, con menor densidad de población, el tamaño de las celdas es mucho mayor, a veces, hasta varios kilómetros, aunque rara vez más de diez kilómetros.[34]

---

[32] TECHOPEDIA (s/f) *¿Qué significa red celular?* [en línea] https://www.techopedia.com/definition/24962/cellular-network [Visto en línea 17/11/2021].

[33] RAMIREZ ZARATE, GUIMER (2014) *Implementación de seguridad domiciliaria mediante comandos AT sobre la tecnología de telefonía móvil.* Memoria para optar al grado de licenciado en electrónica y telecomunicaciones, Facultad de Tecnología Universidad Mayor de San Andrés, Bolivia. p. 14 [en línea] https://repositorio.umsa.bo/xmlui/bitstream/handle/123456789/11564/EG-1369-Ramirez%20Zarate%2C%20Guimer.pdf?sequence=1&isAllowed=y [Visto en línea 18/11/2021].

[34] ORANGE.(s/f) *¿cómo funciona una red móvil? Op. cit.*

El operador de telecomunicaciones instala en las antenas un dispositivo llamado C.D.R. (Call Detail Recorder), registro tasador de llamadas, que almacena información y datos utilizados, principalmente, para llevar a efecto las cobranzas. Entre la información que registra se encuentra la relativa a la radio base, número originador de la llamada, número de destino de la llamada, hora de comienzo, duración de la llamada, tipo de llamada, entre otros.[35]

2. Sistema de georreferenciación del Colegio de Ingenieros de Chile. [36]

A continuación, expondremos las bases de la metodología desarrollada por el Colegio de Ingenieros de Chile a través del profesor Eduardo Costoya, con el fin de utilizarse como medio de prueba para acreditar la participación de los sospechosos de la comisión de un ilícito.

a. Información recopilada del C.D.R.

Gracias a los datos que proporciona el C.D.R., sabemos que un determinado teléfono móvil se encuentra dentro de una zona geográfica determinada. Con todo, dicha área resulta insuficiente para dar exactitud como medio de prueba, puesto que tal área, en caso de ser omnidireccional la cobertura, abarca un perímetro circular bastante extenso, de un radio de cobertura de 1.5 a 2 km en zonas residenciales sin construcciones de altura, y de 500 a 600 metros en zonas de alta densidad con construcciones de altura. La imagen a continuación ilustra el caso.

[35] COLEGIO DE INGENIEROS DE CHILE, Comisión de telecomunicaciones (2019) *Pericia técnica para la causa Rol 1100-2018, RUC 1800078414-8*, 4° Juzgado de Garantía de Santiago.

[36] ibid.

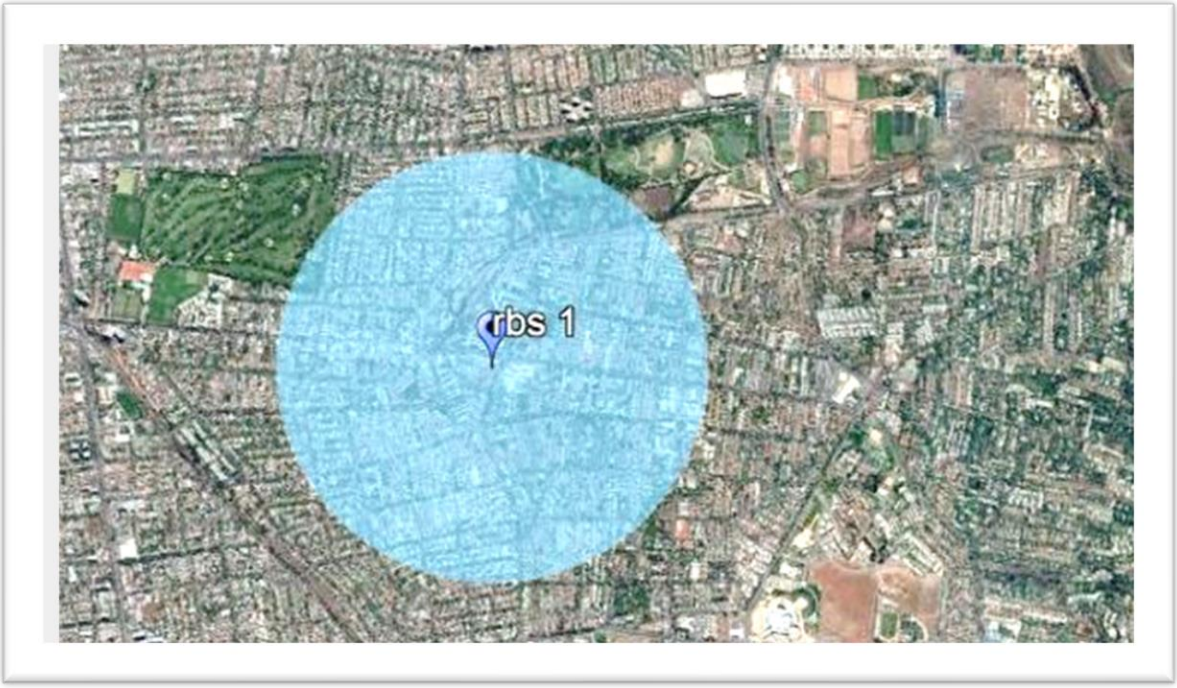

ILUSTRACIÓN 4

Visto esto, si un teléfono móvil se encuentra al azar dentro de esa cobertura, la probabilidad de que se encuentre dentro de una manzana determinada es ínfima, y por tanto insuficiente para utilizarse como medio de prueba dentro de un proceso penal.

Para verificar lo anterior se supondrá que el radio de cobertura en cuestión es de 1000 metros, cubriendo entonces un área de 3.140.000 m2 equivalente a 314 ha, y cada manzana equivaldrá 100x100 metros. Bajo este supuesto, la respuesta sería que la probabilidad de que un teléfono móvil se encuentre dentro de una manzana determinada es de una en 314 (1/314), es decir, 0,32%. Como se ya se mencionó, resulta insuficiente puesto que no con tan baja probabilidad no es posible probar que un teléfono se encuentra dentro de determinada manzana. [37]

b. Existencia de un segundo teléfono celular.

Soslayando el problema de la privacidad de los datos, que será analizado en otro acápite de esta memoria, supóngase ahora que se tiene conocimiento de un segundo teléfono, vinculado a otro

[37] Ibid., p. 7.

sospechoso de la comisión de un ilícito, y que, al haber realizado una llamada, esta se registre en el subsistema de C.D.R de la cobertura de la misma área de comisión del delito, y que a través de la información que registra, pueda verificarse que el teléfono se ubicaba allí en la misma fecha y más o menos a la misma hora.

Ante este nuevo supuesto, la probabilidad de que tal teléfono se encuentre dentro de la manzana en que se cometió el ilícito es idéntica a la primera, es decir, 1/314 o 0,32%.

Ahora bien, la probabilidad de que ambos teléfonos móviles se ubiquen en la manzana en que se cometió el ilícito es aún menor. Dicha probabilidad resulta del cálculo de 1/314 X 1/314, lo que nos da un producto de 1/98,596, es decir, 0,001% de probabilidad.

A partir de esta última probabilidad se puede concluir que para que se produzca dicha confluencia en determinada manzana ambos teléfonos tendrían que estar coordinados para haber estado en ella en un tiempo determinado. [38]

c. Hipótesis de concurrencia de antenas sectoriales.

Como se vio anteriormente, cuando se está en zonas urbanas de mayor densidad, a diferencia de las zonas rurales, se utilizan tres o más antenas sectoriales que cubren toda la zona, con fin de dar la capacidad de llamadas-conexiones que una zona bien poblada requiere. En la imagen a continuación representa la cobertura de una zona, dividida en tres antenas sectoriales.

[38] Ibid., p. 30.

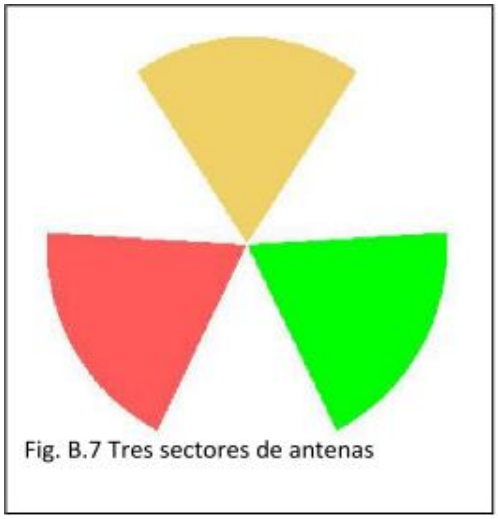

ILUSTRACIÓN 5

Como consecuencia de esta sectorización tenemos que hay un incremento en la probabilidad de establecer la posición de un teléfono al azar, pues la zona en cuestión abarca menor cantidad de manzanas, 105 en específico, según el supuesto en que nos estamos basando. En efecto, la probabilidad de que un teléfono se encuentre en determinado punto geográfico resulta de 1/105; y la probabilidad de que dos teléfonos se hallen en tal punto es de 1/11,025.

Para conocer el sector y el área que éste cubre es necesario requerir más información de los operadores de telecomunicaciones, en específico el **azimut**, lo que proporcionará el ángulo en que se encuentra la antena, utilizando como referencia el norte geográfico.

Según el Eduardo Costoya "en estas condiciones, es necesario complementar lo ya realizado con las coberturas de las celdas para aumentar la precisión de tal modo que se pueda disminuir drásticamente el número de manzanas en la cual pudieran estar ubicado uno o más teléfonos. Este complemento puede ser las técnicas de radiogoniometría, pero modificadas a las condiciones que imponen las coberturas celulares". [39]

Continuando con esta idea, se sostiene que "como se ha expresado anteriormente, la Radiogoniometría permite ubicar con mucha precisión un transmisor de ondas radioeléctricas mediante tres antenas ubicadas en un lugar precisamente determinado, dichas antenas tienen un

[39] Ibid., p. 8.

punto de recepción nulo muy estrecho. Girando las antenas hasta obtener la mínima señal en cada una de ellas, y dado que las ondas radioeléctricas viajan en línea recta, se pueden obtener tres direcciones que determinan en su punto de intersección la ubicación del transmisor. En el caso de la telefonía celular la **situación es la inversa**. Se conoce exactamente la ubicación del transmisor de la señal y lo que se requiere es conocer la ubicación del teléfono que la recibe, el cual, para más complejidad normalmente se está desplazando".[40]

d. Interceptación de áreas.

Al solicitar la entrega de información a los operadores respecto de un determinado número telefónico, se puede poner en conocimiento datos indispensables, que sirven para saber dónde se encontraba tal teléfono móvil en un determinado momento, siempre y cuando haya realizado una llamada, quedando así registro de ella en C.D.R de una estación base. A través de estos datos se puede saber si un sospechoso se encontraba en un área cercana al sitio del suceso donde se cometió un ilícito, pero es de por sí insuficiente para probar que se encontraba con exactitud en el sitio mismo del suceso.

ILUSTRACIÓN 6

En esta imagen tenemos que el punto A corresponde al sitio del suceso. La zona amarilla es el área de cobertura de una antena, la cual captó la señal del teléfono en cuestión, y le permitió realizar una llamada. Entonces, el teléfono móvil pudo hallarse en cualquier punto de la zona amarilla, lo cual muestra un pequeño avance, por cuanto reduce la cantidad de manzanas que se

[40] Ibid., p. 9.

utilizaran para obtener la probabilidad de que al azar se encuentren dos o más móviles en el sitio del suceso.

Pues bien, si tenemos ahora información sobre otro teléfono, que corresponde a otro de los sospechosos, que se encontraba dentro de la misma área del sitio del suceso, y se detecta que realizó una llamada que se conectó, por ejemplo, a otra celda con una ubicación y azimut diferente, y si se produce una intersección entre ellas, dentro de la cual se encuentra el sitio del suceso, se podría entonces reducir aún más la cantidad de manzanas sobre las que va a operar la probabilidad, a la zona en que ambas coberturas confluyen, es decir, su punto de intersección. Suponiendo que los teléfonos están juntos, solo pueden encontrarse dentro de esa zona de intersección.

En suma, la probabilidad de que ambos sospechosos se encontraran al azar en dicha área tan pequeña, en la misma fecha, y en un pequeño lapso es mínima. Lo cual entrega certeza de que ambos se concertaron para reunirse en tal área. Sumando a lo anterior el hecho de que dentro de tal área se encuentra el sitio del suceso de un ilícito del cual ellos son sospechosos, **resultando un indicio que contribuye a determinar y acreditar su participación** en la comisión de un delito.

A continuación, una imagen que ilustra la situación:

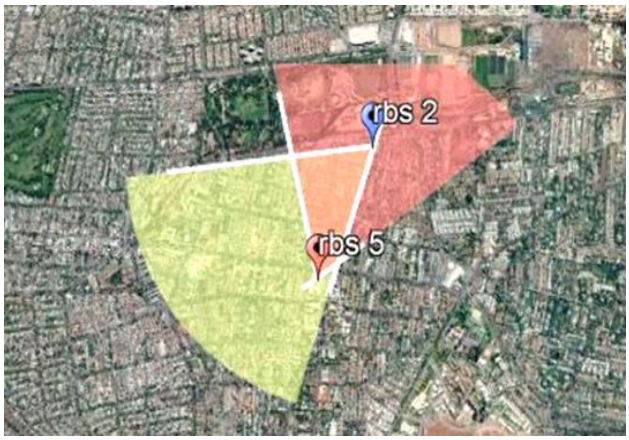

ILUSTRACIÓN 7

Teniendo en cuenta lo anterior, mientras más azimut se hayan conectado con determinados teléfonos, más posibilidades hay de reducir el área en cuestión, a través de la intersección que se produce entre todas ellas. Si se agrega otro teléfono móvil, perteneciente a alguien que

fehacientemente tiene conexión con los otros dos móviles, que fue objeto de otra cobertura, puede reducirse el área en cuestión y, por ende, aumenta la probabilidad de que ubicación de un teléfono móvil.

e. Software utilizado para plasmar la geolocalización.

Para ilustrar la georreferenciación, se ingresan las coordenadas correspondientes dentro de un software que ofrece servicios pagados llamado **Earth Point.us**[41], el cual proyecta los puntos geográficos mediante el sistema de **Google Earth,** cuya precisión se estima que es confiable.

Es conveniente que, dependiendo de la cantidad de llamadas con distintas ubicaciones, las proyecciones sean elaboradas por etapa, para no rellenar de información una sola lámina de la presentación pericial, si no que efectuar varias, de forma sucesiva.[42]

En cuanto a los datos que son necesarios para realizar exitosamente la geolocalización, más adelante nos referimos en detalle a ellos.

f. Conclusión.

En definitiva, este sistema de georreferenciación, complementado con todo tipo de medios de prueba, tales como registros audiovisuales que permitan constatar la ubicación de los sospechosos en una fecha y hora determinada, o bien mediante testigos que aseveren tales circunstancias, permite acreditar la presencia de los sospechosos o imputados de la comisión de un delito en el sitio del suceso.

[41] https://www.earthpoint.us/.

[42] COLEGIO DE INGENIEROS (2019) Op. Cit., p. 9.

Capítulo II. Regulación Jurídica Chilena de la geolocalización a través de utilización de datos de tráfico.

Este capítulo tiene por finalidad analizar los aspectos jurídicos asociados al debido proceso legal, aplicables a la prueba a través de estos medios, permitiéndonos comprender la manera en que opera legalmente el tratamiento de datos de tráfico en Chile.

1. Debido Proceso.

Antes de entrar de lleno en la materia, corresponde esclarecer qué se entiende por debido proceso.

a. Instrumentos Internacionales.

La **Declaración Universal de Derechos Humanos de la ONU** (1948) entrega, en sus artículos N°8 y N°10, una aproximación de lo que ha de comprenderse como debido proceso. El artículo 8 se refiere al derecho al recurso. Más relevante a nuestro es estudio es el artículo 10, que prescribe lo siguiente:

"Artículo 10. Toda persona tiene derecho, en condiciones de plena igualdad, a ser oída públicamente y con justicia por un tribunal independiente e imparcial, para la determinación de sus derechos y obligaciones o para el examen de cualquier acusación contra ella en materia penal."

Cuando el artículo se refiere al derecho a ser oído, debe entenderse que éste comprende el derecho a presentar pruebas que permitan acreditar los hechos. En este sentido, y trayendo los conceptos al caso concreto, la geolocalización es, obviamente, una prueba de la cual se tiene derecho a rendir, como presupuesto del debido proceso.

En segundo lugar, tenemos el **Pacto Internacional de Derechos Civiles y Políticos** (P.I.D.C.P.), de 1966, también de la Asamblea General de la ONU, ratificado por Chile el año 1989, cuyo artículo N°14 estipula que "toda persona tendrá derecho a ser oída públicamente y

con las debidas garantías por un tribunal competente, independiente e imparcial, establecido por la ley […]". De esta manera, se repite lo enunciado en el párrafo anterior respecto del derecho a que sean recibidos los elementos probatorios por el tribunal y sean considerados en su mérito. El mismo artículo consagra el principio de presunción de inocencia, el cual es tremendamente relevante para efectos probatorios, puesto que, en la práctica va a significar que la carga de la prueba va a corresponder a quien acusa la culpabilidad del sujeto.

A nivel regional, contamos con la **Declaración Americana de los Derechos y Deberes del Hombre (1948)**, que en su artículo 18 prescribe que "toda persona puede ocurrir a los tribunales para hacer valer sus derechos". Asimismo, artículo 26 instituye el principio de presunción de inocencia señalando que "se presume que todo acusado es inocente, hasta que se prueba lo contrario."

Finalmente, tenemos la **Convención Americana sobre Derecho Humanos**, también conocida como "**Pacto de San José de Costa Rica**", vigente en Chile desde 1991, que en su artículo 8.1. dispone que "[t]oda persona tiene derecho a ser oída, con las debidas garantías y dentro de un plazo razonable, por un juez o tribunal competente, independiente e imparcial […]."

En definitiva, en el plano internacional, la noción de debido proceso incluye el derecho a ser oído por la judicatura prestablecida, independiente e imparcial.

b. Regulación Nacional.

b.1. Debido proceso chileno en general.

A **nivel nacional**, la Constitución Política de la Republica consagra el debido proceso refiriéndose a un "justo y racional" procedimiento. Las normas esenciales son el artículo 6° (legalidad), el N°3 del artículo 19 (Derecho fundamental), y los artículos 76 y siguientes, (poder judicial).

El inciso 6° del N°3 del Artículo 19 de la Constitución dispone que "Toda sentencia de un órgano que ejerza jurisdicción debe fundarse en un proceso previo legalmente tramitado.

Corresponderá al legislador establecer siempre las garantías de un procedimiento y una investigación racionales y justos".[43]

De la norma del artículo 19 se desprende **el derecho a rendir prueba en juicio** y de que sea valorada por un juez establecido de conformidad con la Constitución. En efecto la rendición de prueba es fundamental en los procedimientos establecidos en la ley. Y, como ha dicho Chiovenda, el "proceso es al procedimiento lo que el agua es al río". [44] Es decir, el procedimiento es la normativa legal en que se sustenta un proceso.

El Profesor **Juan Colombo** define el debido proceso como "aquel que cumple integralmente la función constitucional de resolver los conflictos de intereses de relevancia jurídica con efecto de cosa juzgada, protegiendo y resguardando, como su natural consecuencia, la organización del Estado, las garantías constitucionales y en definitiva la plena eficacia del derecho".[45]

Por su parte, los profesores **Maturana y Montero** definen debido proceso como el "conjunto de normas y garantías que derivan de exigencias constitucionales y tratados internacionales propias del Estado de Derecho, y que como sustento mínimo debe considerar la realización del proceso ante un juez natural, independiente e imparcial, teniendo siempre el imputado el derecho de defensa y derecho a un defensor, la expedita resolución del conflicto, en un juicio contradictorio, en el que exista igualdad de tratamiento de las partes, **pudiendo ambas rendir su prueba,** y el derecho a recurrir la sentencia emanada de éste".[46]

b.2. Derecho a la prueba.

Colombo sostiene que "todo procedimiento, para que sea debido, debe necesariamente otorgar a los sujetos involucrados el derecho a probar los hechos fundantes de sus pretensiones y contrapretensiones y al tribunal, le corresponde valorarla".[47]

---

[43] CHILE. Ministerio Secretaría General de la Presidencia. 2005. Decreto 100: *Fija el texto refundido coordinado y sistematizado de la Constitución Política de la República de Chile*, 22 de septiembre de 2005.

[44] Parafraseado en COLOMBO (2006) Debido proceso constitucional. p.31.

[45] COLOMBO, JUAN. (2006) *El debido proceso constitucional.* Santiago de Chile: Tribunal Constitucional, Cuadernos del Tribunal Constitucional N°32, 2006. p.14.

[46] MATURANA, CRISTIÁN y MONTERO, RAÚL (2010) *Derecho Procesal Penal, tomo I,* Santiago de Chile: Legal Publishing, p.29.

[47] Ibid. p. 105.

El autor **Alex Carocca** se refiere a un verdadero "derecho a la prueba", el que formaría parte del derecho a la defensa. Define el derecho a la prueba como

"la garantía constitucional (o derecho fundamental) que asegura a todos los interesados la posibilidad de efectuar a lo largo del proceso sus alegaciones, sus pruebas y contradecir las contrarias, con la seguridad de que serán valoradas en la sentencia. En definitiva, se trata de la garantía de la participación de los interesados en la formación del juicio jurisdiccional".[48]

En tal sentido, se entiende como contenido mínimo del derecho a prueba el siguiente[49]:

1) Que la causa a prueba sea recibida
2) Existencia de un término probatorio o audiencia para producirla
3) Ofrecimiento de las partes de los medios de prueba de los que dispongan
4) Admisión de la prueba válidamente propuesta
5) Admisión de la prueba practicada
6) Derecho de todas las partes a intervenir
7) Valoración de la prueba por el tribunal

Adicionalmente en el ámbito penal el derecho a la prueba comprende también que tanto el hecho punible como la participación del inculpado sean debidamente acreditados.

La jurisprudencia también se ha referido al derecho de rendición de prueba que envuelve todo debido proceso en una situación en que se le negó presentar prueba al querellado.[50] La Corte Suprema sostuvo que "conforme a la doctrina nacional, el derecho a un proceso previo, legalmente tramitado, racional y justo, […] debe contemplar las siguientes garantías: […] la producción libre de prueba conforme a la ley, el examen y objeción de la evidencia rendida".[51]

---

[48] CAROCCA, ALEX (1998) *Garantía constitucional de la defensa procesal*. Ed. J.M. Bosch, Barcelona, p. 98 y ss.

[49] NARANJO E IBARROLA ABOGADOS (2019) *Aspectos Generales de la Prueba: basado en la separata de Maturana 2015*, p. 11.

[50] Corte Suprema. 11.5.2005. Revista Procesal Penal N° 35. Págs. 55 y Sgtes. Mayo 2005.

[51] C.S., 5 diciembre 2001, R.G.J., 258; Citado en Maturana y Montero [2010] p.31.

A partir de esto se entiende que para recoger la información telefónica registrada en el C.D.R. de una estación base, con la finalidad de presentarla como medio de prueba en un proceso judicial posteriormente, se debe hacer de acuerdo con las normas procesales que el ordenamiento jurídico chileno disponga para el caso.

Otro aspecto relevante de este numeral es el inciso 7° que estipula que la "ley no podrá presumir de derecho la responsabilidad penal", lo cual, como ya se dijo anteriormente, tiene importantísimos efectos en cuanto a la rendición de prueba en juicio y que, en la práctica, se traduce en que la carga de la prueba para acreditar la responsabilidad penal corresponde al Ministerio Público. En nuestro caso, será éste el que debe presentar una prueba pericial acerca de la geolocalización celular efectuada según vimos en la primera parte de este trabajo.

b.3.Conclusiones sobre el debido proceso.

Es aplicable al debido proceso el N°26 del artículo 19, que establece que no puede una ley limitar las garantías de la constitución de forma tal que las afecte **en su esencia** o le imponga condiciones, tributos o requisitos que impidan su libre ejercicio.

Cabe mencionar que existen otros derechos que el debido proceso envuelve y que se extralimitan a los objetivos de este trabajo, como el concepto de juez natural, independiente e imparcial, derecho a la defensa jurídica, derecho a la acción, derecho a expedita resolución del conflicto, publicidad de las actuaciones, entre otros.

De todas maneras, las normas del debido proceso colisionan muchas veces con otros derechos garantizados constitucionalmente, por esto, el derecho a la prueba debe ejecutarse con estricto respeto hacia el resto de los derechos fundamentales, lo cual tiene notable incidencia en relación con las materias tratadas en este trabajo. Respecto de aquellas garantías constitucionales nos referiremos en detalle más adelante.

Esto es así porque el debido proceso es, la mayoría de las veces, consecuencia de un Estado democrático, y que, por lo tanto, implica que derechos y libertades de las personas estén en juego. En consecuencia, "el proceso debe realizarse bajo condiciones especiales de garantía".[52]

[52] MATURANA y MONTERO (2010) *Derecho Procesal Penal.* op.cit.

Por supuesto que la explicación acerca del debido proceso que recién informamos no es más que una parte de este, la que es relevante para efectos de esta Memoria. En consecuencia, se dejan fuera materias de suma importancia tales como el concepto de juez natural, independiente e imparcial, derecho a la defensa jurídica, derecho a la acción, derecho a expedita resolución del conflicto, publicidad de las actuaciones, entre otros.

2. Regulación Legal de las Telecomunicaciones.

2.1. Normativa y artículos relevantes

En nuestro ordenamiento jurídico las telecomunicaciones están reguladas, principalmente, a través de dos normas básicas, a saber, la ley **N°18.168, Ley General De Telecomunicaciones**, y el **Decreto 18, de 13 de febrero de 2014, que Aprueba Reglamento De Servicios Telecomunicaciones.**

Este último entrega ciertas definiciones esenciales para comprender nuestro análisis. En efecto, el reglamento define, en su artículo 2°, lo que se entiende por "**Servicios de telecomunicaciones**", prescribiendo que: "corresponden a todos los servicios que prestan los proveedores de telecomunicaciones, en el marco de lo dispuesto en la ley Nº18.168, de 1982, Ley General de Telecomunicaciones, en adelante la ley, y su normativa complementaria, independientemente del tipo de tecnología utilizada para su provisión, de conformidad a la autorización legal correspondiente."

Por su parte la **Ley General de Telecomunicaciones**, en su artículo 1°, establece que: "Para los efectos de esta ley, se entenderá por telecomunicación toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos e informaciones de cualquier naturaleza, por línea física, radioelectricidad, medios ópticos u otros sistemas electromagnéticos."

A continuación, en lo que interesa define: "Servicios Públicos de Voz: servicios públicos de telecomunicaciones destinados principalmente al intercambio de la voz, tales como: el servicio público telefónico sea local o móvil y los correspondientes servicios públicos del mismo."

El artículo 7° del Reglamento se refiere al **"suscriptor",** definiéndolo como: "Toda persona natural o jurídica que contrata los servicios a que se refiere el presente reglamento o adquiere,

conforme a las normas generales del derecho, tal calidad. Tratándose de los servicios de prepago, se entenderá que ellos revisten la calidad de suscriptores."

A continuación, el artículo 8° define lo que se entiende por **"usuario":** "Toda persona natural o jurídica que hace uso de los servicios de telecomunicaciones a que se refiere este reglamento, incluidos los suscriptores."

Por lo tanto, mientras el suscriptor es la contraparte contractual de la compañía de telecomunicaciones, el usuario es quien emplea los servicios en sus comunicaciones, que es el sujeto protegido por el secreto de las comunicaciones, pero también el responsable del contenido de éstas. No obstante, normalmente suscriptor y usuario coinciden, no siempre será así por lo que en cada caso se debe confirmas la persona de uno y otro sujeto.

Otra definición importante para este trabajo, la encontramos en el artículo 4° del Reglamento: "Artículo 4º. Equipo Terminal: todo equipo que interactúa directamente con el suscriptor y/o usuario permitiéndole transmitir y/o recibir voz, datos, imágenes, video y/o información de cualquier naturaleza, a través de las redes de telecomunicaciones y aplicaciones que sobre dicha red se soportan y a cuyo contenido las funcionalidades del equipo permitan acceder, tales como **equipos telefónicos móviles y de telefonía local, computadores, aparatos de televisión** y cualquier otro equipo que constituya la interfaz con el usuario. Estos equipos deben cumplir con las normas de homologación que les sean aplicables." (El énfasis es nuestro).

Finalmente, nos encontramos frente al artículo 24 del Reglamento, de suma importancia, puesto que se refiere a la utilización de datos personales de los suscriptores y usuarios, en los siguientes términos: "Artículo 24º. Los datos personales de suscriptores y usuarios recabados por los proveedores de servicios de telecomunicaciones con motivo de la contratación y suministro de los servicios de telecomunicaciones regulados en el presente Reglamento, sólo podrán utilizarse para los fines específicos asociados a la prestación del servicio, debiendo someterse en el tratamiento de tales datos a lo previsto al efecto en la Ley Nº19.628, Sobre Protección de la Vida Privada." Tema al que nos referiremos más adelante en esta monografía.

2.2. Ausencia de definición de datos de tráfico.

Habiendo analizado toda la normativa relativa a telecomunicación, en general, y sus reglamentos particulares, notamos que no hay en ninguno de ellos una definición de datos de tráfico

3. Ley 19.628. Sobre Protección de la Vida Privada.

Esta ley **regula el tratamiento de datos personales**, aunque de manera notablemente insuficiente, considerando la masificación del uso de datos personales durante la última década, no se ha adecuado a los estándares legislativos internacionales, que son naturalmente más rigurosos. La ley fue publicada el año 1999, y ha sido objeto de **ínfimas modificaciones**, materializadas a través cinco leyes. Su última modificación es de 28 de febrero de 2020, correspondiente a la llamada Ley "Chao DICOM".[53]

El **artículo 2°** hace una distinción entre **dato estadístico y datos personales,** definiendo el primero como "el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable".[54] Por su parte, son **datos personales** "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables".[55] Estas definiciones son relevantes al objeto de nuestro estudio porque entre los datos derivados de los servicios de telecomunicaciones necesarios para llevar adelante el método investigativo que analizamos encontraremos datos de ambos tipos.

El **artículo cuarto** prescribe que el tratamiento de los datos personales solo puede efectuarse cuando esa ley u otras disposiciones legales lo autoricen o el titular consciente expresamente en ello. Sin perjuicio de lo anterior, el **inciso segundo del artículo primero** prescribe que "toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico".

---

[53] BIOBÍO (2020) Entra en vigencia ley "Chao Dicom": encargados de registros tendrán 6 meses para adecuarse [en línea] <https://www.biobiochile.cl/especial/educacion/noticias/2020/03/02/entra-en-vigencia-ley-chao-dicom-encargados-de-registros-tendran-6-meses-para-adecuarse.shtml> [Visto en línea 10/04/2020].

[54] Ley 19.628 art. 2 letra f).

[55] Ley 19.628 art. 2° letra g).

Luego, el inciso final dispone que no se requerirá de autorización en casos de tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos.

En todo caso el responsable del banco de datos deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.

Las empresas de telecomunicaciones tratan los datos personales necesarios para la provisión de sus servicios: Los datos de abonado le permiten poblar y administrar su base de datos de clientes, los datos relativos a comunicaciones iniciadas en las cuentas de usuario se emplearán en los procesos de facturación; los datos de morosidad serán empleados en los procesos de cobranza, por mencionar algunos de los tratamientos de datos que realizan estas compañías. La fuente legal de este tratamiento la encontramos en la ley General de Telecomunicaciones, su reglamento y adicionalmente, los contratos de suscriptor incluyen cláusulas de autorización.

El **artículo 6°** prescribe que "los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado."

En nuestro caso el fundamento legal para la conservación se encuentra en el **artículo 222** del C.P.P. al establecer un plazo mínimo de un año, no obstante, de que no imponga un plazo máximo, lo cual se verá en detalle más adelante. Junto con esto, el **artículo 11** establece la obligación de cuidar los registros de datos personales con la debida diligencia, haciéndose responsable de los daños.

Por su parte, el **artículo 9°** dispone que los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados. En este sentido, se les prohíbe a las empresas de telecomunicaciones utilizar los datos para otros propósitos distintos al de tarificación.

3.1. Datos de tráfico en la ley de protección de datos personales.

Ahora bien, la ley Sobre Protección a la Vida Privada tampoco **no nos entrega una definición de datos de tráfico**, aunque puede subsumirse dentro de la categoría de dato estadístico o de dato personal según cuál sea la naturaleza individual de cada uno de los datos de tráfico.

Así, por ejemplo, el IMEI del equipo terminal –teléfono celular en nuestro caso- cabría dentro de la categoría de **dato personal,** puesto que a partir de él se puede llegar a conocer la identidad de la persona usuaria del equipo. Aun así, hay que distinguir, puesto que en los casos de servicio prepago no será posible dar con la identidad del usuario, toda vez que ésta no está vinculada con el equipo terminal. De hecho, la delincuencia organizada está al tanto de esta situación, por lo que la utilizan a su favor para evitar que la policía llegue a dar con su identidad al momento de, por ejemplo, interceptar las comunicaciones telefónicas de un número del cual tengan conocimiento y sospechas de que el mismo corresponda a alguien que participó o participará en la comisión de un delito. Asimismo, entra en la categoría de dato personal, la información sobre las llamadas o comunicaciones cursadas desde o hacia la línea de abonado, que luego serán incluidas en los procesos de facturación.

Al contrario, se trataría de **datos estadísticos** cuando a partir de ellos no pueda establecerse la identidad de su titular; que es lo que sucede, por ejemplo, con la información acerca de la duración de las llamadas telefónicas, su fecha y hora, si se trata de una llamada de entrada o de salida, entre otros.

Como analizaremos más adelante, hoy está en trámite un proyecto de ley que propone una definición más o menos acabada de "datos relativos a tráfico".[56]

4. Convenio de Budapest Sobre Ciberdelincuencia.

A través del Decreto N° 83, de 28 de agosto de 2017, del Ministerio de Relaciones Exteriores, se incorporó a nuestro ordenamiento jurídico el Convenio sobre Ciberdelincuencia, más conocido como "Convenio de Budapest", que fue suscrito el 23 de noviembre de 2001. En sus normas, el Estado de Chile se compromete a regular o tipificar determinados delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos [Título I]; delitos informáticos tales como falsificación, fraude [Título II]; delitos relacionados con el contenido, como delitos relacionados con pornografía infantil [Título III]; y delitos relacionados con infracción de la propiedad intelectual y de los derechos afines [Título IV].

[56] Ver capítulo III. 7.1.

En cuanto a lo que nos interesa, el Convenio, en su artículo 1° letra d), **define "datos relativos a tráfico",** "a los efectos" del Convenio, en los siguientes términos: "d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente."

Si bien la definición se refiere a información proveniente de un sistema informático (no un sistema de telefonía), entendemos que esta definición resulta aplicable al objeto de nuestro estudio, sobre todo si consideramos que las redes de telecomunicaciones están digitalizadas.

En todo caso, el artículo 5° de la Ley General de Telecomunicaciones dispone que "el significado de los términos empleados en esta ley y no definidos en ella, será el que le asignen los convenios internacionales sobre telecomunicaciones vigentes en el país".

En el ámbito doctrinario, el profesor **José Julio Fernández Rodríguez, de la Universidad de Santiago de Compostela**, "los datos de tráfico, o metadatos, en una comunicación son los datos que rodean el mensaje que se transmite, pero que no forman parte de dicho mensaje". [57]

Más adelante volveremos sobre estas materias.

5. Normativa Procesal Penal.

a. Artículo 222 CPP.

Si bien el Código Procesal Penal no regula de manera expresa y específica el tratamiento de datos relativos a tráfico en las investigaciones penales, la doctrina y la jurisprudencia se han remitido al artículo 222 de dicho cuerpo legal, referido a la interceptación de las comunicaciones, no obstante tratarse de técnicas diferentes. Si analizamos este artículo observamos que su inciso primero no limita su alcance a la telefonía, sino que señala expresamente que en las hipótesis que se señalan, "el juez de garantía, a petición del ministerio

[57] FERNÁNDEZ, JOSÉ JULIO (2016) Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente. Revista Española de Derecho Constitucional, volumen 108 (p. 93- 122), p. 96.

público, podrá ordenar la interceptación y grabación de sus comunicaciones telefónicas o de otras formas de telecomunicación".

En lo que se refiere a los datos que son objeto de tratamiento por las compañías telefónicas, el artículo 222, inciso 5° prescribe lo siguiente: "Las empresas telefónicas y de comunicaciones deberán dar cumplimiento a esta medida, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera. Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento".[58] Se ha entendido que en virtud de lo dispuesto en este artículo, la empresa de telecomunicaciones requerida debe proporcionar información referente a datos de tráfico y a los números telefónicos, siempre que dicha solicitud se realice en conformidad con el debido proceso.

En **segundo lugar**, la disposición legal obliga a las empresas de telecomunicación a mantener un **listado actualizado de sus rangos autorizados de direcciones IP** y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados. Si bien la norma no hace mención expresa de datos relativos a tráfico o asociados, se ha interpretado que la obligación de conservación se extiende a éstos.

Se cuestiona el hecho de que se establezca sólo un plazo mínimo de conservación de los datos (1 año) y no un plazo máximo, porque deja esta materia al arbitrio de las empresas de telecomunicaciones, lo cual resta certeza jurídica. A vía ejemplar, el proveedor WOM publica que "mantendrá registro de los metadatos de comunicaciones de sus clientes en cumplimiento

[58] Artículo 222 CPP.

legal. Es así como luego de 2 años estos datos serán eliminados, de acuerdo a parámetros técnicos para asegurar su eliminación segura y la reserva de la misma".[59]

En tercer lugar, el artículo 222, inciso 5°, prescribe que la negativa o el entorpecimiento a proporcionar la información por parte de las empresas operadoras de telecomunicaciones, podrá castigarse como delito de desacato.

b. Autorización judicial.

Como vimos antes, en atención a que los datos de tráfico pueden incluir datos personales protegidos por la garantía fundamental en el artículo 19 N°4 de la C.P.R., además de los otros derechos constitucionales, aplicando los artículos 222 y 9° del C.P.P[60], se desprende la necesidad de orden judicial previa del juez de garantía para recabar información.

Pablo **Viollier** —en su rol de miembro de la ONG "Derechos Digitales"— ha señalado que "la orden judicial previa es un requisito necesario no solo para la interceptación de comunicaciones, sino que también para solicitar la entrega de metadatos".[61] A ello agrega que incluso "las empresas interpretan que el acceso a los datos de tráfico (o metadatos), establecido en el inciso quinto del artículo 222 del Código Procesal Penal, requiere de una orden judicial previa".[62]

Siguiendo con el ejemplo de la empresa WOM, en sus políticas cuenta con un "Protocolo de entrega de información a la autoridad", que incluye la información de cómo solicitar información y sus requisitos. En lo que se refiere a datos de tráfico, indica que el Fiscal del Ministerio Público, PDI o Carabineros de Chile deberán adjuntar una Resolución Judicial debidamente firmada y timbrada, junto con los "datos mínimos del requerimiento, tales como RUC de la investigación, tribunal, fecha de la autorización, número objetivo y periodo".

---

[59] WOM (2020) *Protocolo de entrega de información a la autoridad año 2020* [en línea] p. 4 <http://www.wom.cl/bases/bases/documents/Protocolo-Entrega-Informaci%C3%B3n-Autoridad.pdf> [Visto en línea 16/04/2020].

[60] Artículo 9 CPP: "toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de autorización judicial previa"

[61] VIOLLIER, PABLO (2019) ¿Quién defiende tus datos? [en línea] Derechos Digitales América Latina ONG. p.28 <https://www.derechosdigitales.org/wp-content/uploads/quien-defiende-tus-datos-2019.pdf> [Visto en línea 25/10/2019].

[62] Ibid. p.54.

Además, agrega al pie de página de su versión 2020 que "en el caso que solicite además del tráfico, la georreferenciación de las celdas o cualquier combinación de las anteriores deberá acompañar la Resolución Judicial firmada, donde se indique explícitamente lo solicitado".[63]

De ello deducimos que la empresa entiende que no basta una autorización genérica sino que debe contener todos los detalles asociados a la diligencia.

La empresa VTR también establece la exigencia de adjuntar una orden judicial previa, para los requerimientos de datos de tráfico, incluso cuando se trate de casos de tramitación urgente.[64]

Similar es el caso de Claro, en que la "autoridad debe contar con una orden judicial previa, emanada de un Tribunal de la República, en la que se identifique específicamente el tribunal que emite la resolución, la causa con número de RUC o RIT y se individualice claramente al usuario o cliente, la cual deberá siempre adjuntarse al requerimiento. Por otro lado, se exige que sea el Fiscal de la causa y no otro individuo quien realice la solicitud a un correo electrónico especialmente señalado para tal efecto".[65]

b.1. Solicitud del Ministerio Público.

Naturalmente, la orden judicial está precedida por la solicitud que debe hacer el Ministerio Público al juez competente para que autorice la correspondiente diligencia; que deberá incluir expresamente lo que se pide, entregando fundamentos de hecho y de derecho para ello.

En general, se ha recomendado que la solicitud contenga lo siguiente:[66]

- Especificación del delito o crimen acreditando mediante antecedentes su gravedad para fundamentar su procedencia.

[63] WOM (2020) Op. Cit. p.3.

[64] VIOLLIER. (2019) Op.Cit. 39p.

[65] Ibid. p.49.

[66] CANALES, MARÍA PAZ; LARA, JUAN CARLOS (2018) *La construcción de estándares legales para la vigilancia en América Latina Parte III: propuesta de estándares legales para la vigilancia en Chile.* Santiago de Chile: Derechos Digitales. p19.

- Especificación de las personas estrechamente vinculadas con el delito o crimen investigado, dando explicación de tal vinculo, mencionando las evidencias que lo acrediten.
- Individualizar la información que se pretende obtener a través de la autorización judicial, relacionándola con los hechos acontecidos, especificando con exactitud cada una de las peticiones, mencionando las evidencias que permitan justificar la autorización de la medida.
- Detallar el procedimiento al que será sometida la información recabada, señalando el formato con que se presentará en juicio. Especificando "protocolos de custodia, acceso, resguardo, respaldo y eventual eliminación de la información recolectada y sus respaldos, incluyendo a las personas o instituciones involucradas en la ejecución de la medida".[67]
- Dar explicaciones de por qué se hace necesaria la medida en vez de otras que podrían tomarse, demostrando que éstas serían inútiles.

Ahora, en el caso concreto, tales diligencias se traducen en que la solicitud que presente el fiscal ante el juez, para que éste posteriormente autorice tal diligencia, debe contener lo siguiente:

- En primer término, se debe indicar cual o cuales son las empresas de telecomunicaciones a que se va a dirigir la orden.
- Toda información relativa a las coordenadas geográficas de la radio estación, su latitud y longitud, preferentemente en grados decimales, incluyendo dirección, comuna y región. Además, indicar su código de soporte y a qué compañía de telecomunicaciones pertenece.
- Se solicita la entrega de registros no tasables, respecto de tráfico de voz, datos y SMS, junto con la entrega de los *call detail record* [C.D.R], que contengan la integridad de los registros contenidos en la central telefónica.

En concreto, se trata de lo siguiente:

1. Número de teléfono investigado.

[67] Ibid.

2. Número de teléfono corresponsal.
3. **IMEI**. Es la sigla en inglés para *International Mobile Station Equipment Identity*. El IMEI es un código que consta de 15 dígitos, el cual se utiliza para identificar a nivel mundial cada equipo móvil, y que es otorgado por el fabricante al momento de producirlo. Los IMEI poseen un código para identificar tanto la marca como el modelo, el cual es entregado a los fabricantes de todo el mundo por la GSMA (*Global System Mobile Association*).[68] En la práctica se autoriza judicialmente por el plazo de 60 días que se estipula para interceptación de telefonía.
4. Indicar si se trata de una llamada de entrada o de salida.
5. Si la llamada es de voz o de datos, puesto que si es de datos no hay manera de conocer el número de teléfono corresponsal.
6. Día del comienzo de la llamada, especificando año, mes y día. (Año, mes y día).
7. Hora del comienzo de la llamada, especificando minutos y segundos.
8. Hora de término de la llamada, con las mismas especificaciones que arriba.
9. Duración de la llamada en segundos.
10. Celda utilizada.
11. Azimut de la celda.
12. Modelo de la antena o características técnicas, con especial mención del ancho del lóbulo principal en grados.
13. Ganancia de la antena.

Por supuesto, como ya se señaló, la solicitud debe entregar **fundamentos concretos** que se condigan con el principio de proporcionalidad de la medida, para que el juez tenga en consideración al momento de ordenar o denegar la autorización para requerir tal información.

[68] ENACOM (s/f) ¿Qué es el IMEI? [en línea] <https://www.enacom.gob.ar/imei> [Visto en línea 10/04/2020].

b.2. Autorización Fundada del Juez.

El juez debe analizar de manera previa la idoneidad, necesidad y proporcionalidad de la medida y dictar una resolución fundada justamente por el hecho de que se limitan derechos fundamentales y porque el afectado no puede impugnarla en el momento en que se decreta.

En efecto, la doctrina ha recomendado "fundamentar la decisión sobre el otorgamiento de la autorización, en función del análisis de los antecedentes presentados en la solicitud de autorización y debido a la legalidad, necesidad, idoneidad y proporcionalidad de la medida solicitada en relación con los hechos investigados".[69]

En el mismo sentido, Alejandro Ivelic sostiene que el "control judicial sobre las interceptaciones telefónicas se justifica en la medida que esta diligencia investigativa restringe o limita derechos fundamentales y además no es posible que al momento de su adopción el sujeto pasivo de la misma pueda ejercer el derecho a su impugnación. Es por ello que para hacer efectivo el control judicial sobre la diligencia, se requiere que en le resolución que la autoriza se hagan constar la existencia de los indicios que justifiquen la injerencia, su necesidad e idoneidad".[70]

Cierto es que el autor se está refiriendo a la interceptación de las comunicaciones. No obstante, sus conclusiones pueden extrapolarse al tratamiento de datos de tráfico, puesto que este también supone una vulneración de derechos fundamentales, aunque lo sea con menor intensidad.

En la resolución se determina su alcance, haciendo indicación de "los nombres o números de cuentas de servicios de comunicación o de almacenamiento de datos, o los dispositivos o sistemas informáticos a que se refiere; el método particular de vigilancia o recolección de información autorizado, y el período de tiempo a que se extiende la medida".[71]

Adicionalmente, será mención esencial el **periodo durante el que pueda estarse en posesión** de la información recolectada, de forma tal que no sea utilizada para otros fines.

---

[69] Ibid. p. 20.

[70] IVELIC, ALEJANDRO. (2014) *Las interceptaciones de comunicaciones telefónicas en los delitos de tráfico ilícito de estupefacientes*. Revista Jurídica del Ministerio Público. N° 60, septiembre 2014. p. 112.

[71] CANALES & LARA (2018) op.cit. p. 21.

Una vez autorizada la medida, se recomienda al solicitante informar al juez acerca del proceso de recolección de los datos y el cumplimiento de los "protocolos de acceso, custodia y eliminación".[72]

b.4. Proporcionalidad de la medida.

La ponderación es, tal como su nombre lo indica, un ejercicio intelectual que debe realizar el juez que conoce del asunto, que se traduce en poner en una balanza, hipotéticamente, dos derechos que se hallan en contradicción, de forma de medir cuál, en el caso concreto, ha de preponderar sobre el otro. Así, se sopesan los distintos intereses del conflicto, en especial el interés público en contraposición con el interés del titular del derecho fundamental, debiendo establecer cuál será el que deberá primar en cada caso en concreto.[73] Si bien la proporcionalidad no se encuentra consagrada expresamente en la Constitución ni en la ley, entendemos que la exigencia emana de la existencia de un Estado de Derecho y la interdicción de la arbitrariedad de los poderes públicos[74].

Tratándose de la materia en estudio, confluyen el interés del Estado de resguardar la paz social y la investigación de los delitos, que se contrapone al interés del sospechoso en que se reconozca y resguarde los derechos fundamentales a la protección de datos, y al secreto de las comunicaciones, entre los que hemos señalado antes.

El principio de proporcionalidad contiene tres elementos:

a. **Idoneidad**. Es la aptitud para lograr el fin que se persigue, cual es investigar y probar los hechos que se investigan y la participación de los agentes.

b. **Necesidad**. Dice relación con que no exista otro medio menos gravoso para conseguir el fin perseguido, entendiéndose por gravoso el que restrinja derechos fundamentales.

c. **Proporcionalidad en sentido estricto**. Análisis concreto del juez respecto al grado real de afectación del derecho y la gravedad del delito investigado. [75]

---

[72] Ibid.

[73] Ibid.

[74] Ibid. P. 113.

[75] Ibid.

b.5. Notificación al afectado.

El artículo 224 del C.P.P. establece la obligación de notificar al afectado sobre la medida o diligencia con posterioridad a su realización, en cuanto el objeto de la investigación lo permitiere, y en la medida que ello no pusiere en peligro la vida o la integridad corporal de terceras personas; remitiéndose en lo demás al artículo 182, el cual regula el secreto de las actuaciones de investigación, tal como su título dice. Al respecto, incumbe referirse a su inciso tercero; que dispone que "el fiscal podrá disponer que determinadas actuaciones, registros o documentos sean mantenidas en secreto respecto del imputado o de los demás intervinientes, cuando lo considerare necesario para la eficacia de la investigación". Es así como el artículo 236 del CPP establece una **excepción** a la obligación de notificar cuando "la gravedad de los hechos o la naturaleza de la diligencia de que se tratare permitiere presumir que dicha circunstancia [no notificar] resulta indispensable para su éxito", que puede aplicarse con anterioridad y posterioridad de la formalización de la investigación.

Consecuente con lo anterior, estimamos relevante que, al solicitar la autorización de la medida o con posterioridad a su realización, se fundamenye la necesidad de que se mantenga el "secreto de las actuaciones de investigación".[76]

6. Decreto 142 de 2005: Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación.

El artículo 6° de este reglamento regula la obligación de los operadores de mantener un registro de los números IP de las conexiones de sus abonados, estableciendo un plazo mínimo de conservación de seis meses, tiempo menor que el normado en el inciso quinto del artículo 222 del Código Procesal Penal.

La diferencia se explica porque hasta 2011, el C.P.P. establecía una conservación de mínimo seis meses, lo que fue modificado por la ley 20.526, que sanciona el acoso sexual de menores, la pornografía infantil y la posesión de material pornográfico infantil. Asimismo, debemos tener en cuenta que el Decreto en análisis está dirigido a proveedores de acceso a Internet, mientras

[76] CANALES & LARA (2018) Óp.. Cit. p. 21.

que el 222 utiliza términos más generales, dirigiéndose a las empresas telefónicas y de comunicaciones.[77]

Sin perjuicio de lo anterior, en lo que nos interesa, estimamos que prima el plazo de un año establecido en el CPP, por tratarse de una norma de rango legal.

7. Procedimientos posteriores a la recolección de datos.

a. Cadena de custodia.

En Chile no existe una definición legal de cadena de custodia, por lo que, para los efectos de nuestra investigación hemos considerado el siguiente concepto, elaborado por el Tribunal Supremo Español que entiende que es tal un "Conjunto de actos que tienen por objeto, la recogida, traslado, conservación de los indicios y vestigios obtenidos en el curso de la investigación criminal, actos que deben cumplimentar una serie de requisitos con el fin de asegurar la autenticidad, inalterabilidad e indemnidad de las fuentes de prueba"[78]

La cadena de custodia permite dejar constancia del tratamiento que tuvo la evidencia desde el momento en que se recogió, por ejemplo, saber quién la ha tenido en sus manos antes de presentarse en el proceso como medio de prueba. Asimismo, permite dar garantía al Juez de que el material recolectado es el mismo que se ha sometido al análisis del perito y el mismo que se presenta el día del juicio.[79]Es decir, garantiza que la evidencia no fue manipulada indebidamente durante el proceso[80].

Dicho en otros términos, la cadena de custodia tiene tres finalidades esenciales:

---

[77] CHILE (2005) Ministerio de transportes y telecomunicaciones. Decreto 142/2005: Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación. Publicado el 22 de septiembre de 2005.

[78] NATAL MARCOS, NATALIA (2020) *La cadena de custodia: algunos problemas específicos de exclusión probatoria.* Facultad de Derecho Universidad de León p. 18.

[79] DE AGUILAR GUALDA, SALUD (2019) *La prueba digital en el proceso judicial. Ámbito Civil y Penal.* [en línea] Barcelona: Botsch Editor. Disponible en https://www-digitaliapublishing-com.uchile.idm.oclc.org/visor/62844 [Visto en línea 10/10/2020] p. 22-23.

[80] GARCÍA MATEOS, JOSÉ AURELIO. 2016. Cadena de custodia vs mismidad. Disponible en: La prueba electrónica, validez y eficacia procesal. Colección Desafíos legales Juristas con Futuro. 131p.

1. Garantizar la indemnidad de la prueba.
2. Evitar alteraciones, sustituciones, contaminaciones o destrucciones.
3. Dar certeza que la evidencia que se presenta al tribunal es aquella que fue recolectada.[81]

Esto último es lo que se conoce como **Principio de Mismidad,** que es una forma de garantizar que "aquello con lo que se trabaja es lo mismo que aquello que se intervino."[82]

Es así como se ha dicho que "lo determinante en la cadena de custodia pasa por la diligencia profesional de cada uno de sus intervinientes y su fiabilidad depende, en buena medida, de la honestidad del testimonio de los participantes en la misma".[83] Además de los registros documentales, cada uno de los intervinientes debiera referirse al momento, el estado y de quien recibió el objeto, además de las condiciones asociadas a la devolución o entrega de forma que sea susceptible de advertir posibles errores o falseamientos[84], que pudieran derivar en una prueba que vulnera el "derecho a un proceso justo con todas las garantías", lo que se traduciría en un caso de "prueba prohibida".[85]

Se ha sostenido que la cadena de custodia consta de las siguientes etapas:

1. Extracción y obtención de la prueba.
2. Preservación de la prueba.
3. Traslado de la prueba.
4. Análisis y presentación de la prueba a las partes.
5. Custodia y preservación de las pruebas hasta la realización del juicio oral.[86]

El resguardo de la cadena de custodia corresponde, la mayoría de las veces, al Ministerio Publico, puesto que son ellos quienes recolectan las evidencias respectivas. Así, en nuestro caso

---

[81] GARCÍA MATEOS. 2016. Op.cit. p. 131.

[82] Íbid.

[83] GONZÁLEZ I JIMÉNEZ, ALBERT (2014) *Las diligencias policiales y su valor probatorio.* Barcelona: Botsch Editor. P 275.

[84] Ibid.

[85] Ibid. 281.

[86] LÓPEZ BETANCOURT, EDUARDO (2017) *Juicios orales en materia penal.* México: Iure Editores, p. 119.

concreto, les corresponde custodiar la información obtenida del C.D.R. de la estación base, de forma que se garantice el principio de mismidad.[87]

En todo caso, al tratarse de información proporcionada por las empresas de telecomunicaciones a través de documentos (planilla Excel o documento Word), la cadena de custodia consistirá en la constatación de que la información con que se desarrolló la geolocalización se condiga con la proporcionada por tales empresas y que no se han alterado los registros. En caso de que no se detecten anomalías se tendría por cumplido el principio de mismidad.

A estos efectos, resultaría de utilidad que el documento enviado por las empresas de telecomunicaciones se suscriba con **firma electrónica avanzada**, toda vez que da certeza sobre su contenido frente a posibles futuras alteraciones. Al respecto, la **letra g) del artículo 2° de la ley N°19.799** [88] define la firma electrónica avanzada como "aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría." De esta forma, la firma electrónica avanzada permite que sea detectada cualquier modificación posterior en cuanto al contenido de un documento.

b. Informe de peritos.

La persona apta para manipular información de datos de tráfico con el propósito de elaborar la correspondiente georreferenciación es un experto en el área de las telecomunicaciones, mediante un peritaje o informe de peritos. **Casarino** define al perito como "toda persona que tiene conocimientos especiales sobre una materia determinada y apta, en consecuencia, para dar su opinión autorizada sobre un hecho o circunstancia contenida en el dominio de su competencia".[89]

---

[87] Ibid. p 279.

[88] CHILE. Ministerio de Economía, fomento y reconstrucción. *Ley N°19.799: Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.* Publicada el 12 de abril de 2002.

[89] CASARINO VITERBO, MARIO (1984) *Manual de Derecho Procesal, tomo IV, cuarta edición.* Santiago de Chile: Editorial Jurídica de Chile. p. 189.

Los **peritos** "son terceros ajenos al juicio que procuran a los jueces el conocimiento del cual éstos carecen, referido a una determinada ciencia o arte".[90]

El **informe de perito**, en cambio, ha sido definido como "la opinión escrita emitida en un proceso, por una persona que posee conocimientos especiales de alguna ciencia o arte, acerca de un hecho sustancial, pertinente y controvertido o de alguna circunstancia necesaria para la adecuada resolución de un asunto".[91] **Casarino** lo ha definido como "la presentación al juicio de un dictamen u opinión sobre hechos controvertidos en él, para cuya adecuada apreciación se requieren conocimientos especiales de alguna ciencia o arte".[92] Es a través de la observación y análisis de los hechos y fuentes de prueba, que el perito es capaz de deducir o extraer conclusiones de carácter técnico o científico.

Atendida la relevancia del perito, en la formación de la comprensión y convicción del tribunal, además de los conocimientos técnicos (sobre telecomunicaciones) debe estar dotado de gran capacidad para darse a entender lo más claro posible.

La doctrina hace una **distinción entre testigo, testigo-perito y perito**. La diferencia que existe entre los dos últimos radica en que los primeros son los que "declaran sobre lo que ellos han observado con motivo de su conocimiento profesional especial".[93] **Roxin** ilustra este tipo de peritos utilizando el caso de un médico que constata que cierta mujer está embarazada de 4 meses.[94] En cambio, el perito propiamente tal es quien contribuye con el fiscal o el tribunal en cuanto posee conocimientos sobre principios de la ciencia o reglas de arte u oficio, y las aplica para apreciar un hecho o circunstancia relevante en una causa y opinar sobre las circunstancias específicas en que pudo gestarse el resultado que se observa.

Los testigos peritos se rigen por las normas relativas a la prueba testimonial, mientras que los peritos, naturalmente, por las normas sobre prueba pericial, sin perjuicio que en cuanto a la forma en que declaran todos ellos se rijan por las normas de los testigos.

---

[90] BUENO DE MATA (2014) op. cit. N°71, p. 520.

[91] MATURANA; MONTERO (2010) Derecho Procesal Penal, Tomo II. Editorial Legal Publishing, Chile, p. 1030.

[92] CASARINO (1984) op. cit. N°78. p.189.

[93] MATURANA; MONTERO (2010) op.cit. p. 1032-1033.

[94] ROXIN, CLAUS (2000) Derecho Procesal Penal. Editores del Puerto. Buenos Aires. Traducción 25° edición alemana. P. 220.

En la práctica, los peritos se hacen presentes en el proceso de dos maneras: primero a través de un informe de carácter imparcial, que debe regirse por los principios y reglas propios de la ciencia, arte u oficio que aquellos practiquen; y segundo, a través de su declaración en el juicio oral, ya sea bajo juramento o bajo promesa de decir verdad.

La regulación de los peritos se encuentra en el párrafo 6°, del Título III, del libro II del Código Procesal Penal; artículos 314 a 322.

A partir del tenor del **artículo 314**, que se refiere a la **procedencia del informe**, se pueden desprender las siguientes reglas:

1. Procede el informe de peritos cuando: (1) así lo determine la ley; (2) siempre que para apreciar algún hecho o circunstancia relevante para la causa fueren necesarios o convenientes contar con conocimientos especiales de una ciencia, arte u oficio. Entonces la prueba pericial puede ser obligatoria, cuando la ley lo determina, y facultativa, en el caso (2). En el caso que nos concierne, se trata, evidentemente, de una pericia facultativa.
2. El informe debe solicitarse en la audiencia de preparación del juicio oral, pues en ella es donde se discute acerca de los medios de prueba.
3. Debe acompañarse comprobante que acredite la idoneidad profesional del perito, por ejemplo, título profesional relacionado con las ciencias o artes que se requieran en cada caso concreto. Entonces, la idoneidad deberá analizarse en cada caso concreto. Por ejemplo, en el caso que nos ocupa, serán idóneos los peritos con conocimientos en el área de las telecomunicaciones.
4. Debe existir imparcialidad en el informe del perito, ateniéndose a los principios de la ciencia o reglas del arte u oficio que profesare el perito.

El **artículo 315** se refiere al **contenido del informe de peritos**. En lo que concierne a este trabajo las siguientes reglas son relevantes:

1. Contener la descripción de la persona o cosa que fuere objeto del análisis, del estado y modo en que se hallare. Esta descripción supone llevar a cabo el procedimiento de **reconocimiento,** a través del cual el perito conoce y recopila antecedentes mediante actuaciones (320 CPP). Así, en nuestro caso, debe describirse qué es un C.D.R., las

estaciones base en las cuales quedaron registros, las fechas, y los archivos que han sido objeto de análisis.

2. La relación circunstanciada de todas las operaciones practicadas y su resultado; desde la obtención de los archivos y luego explicar el procedimiento de georreferenciación al que ya nos referimos, de forma cronológica, con la finalidad de dejar claro cómo se llegó a la ubicación de los teléfonos móviles.
3. Las conclusiones que, en vista de tales datos, formularen los peritos conforme a los principios de su ciencia o reglas de su arte u oficio. A vía ejemplar, que existe una alta probabilidad de que los imputados se encontraban en el sitio del suceso, conforme se desprende del análisis de los registros de que se trate.

A continuación, el **artículo 316** regula la **admisibilidad del informe y la remuneración** de los peritos:

1. Corresponde al juez de garantía declarar la admisibilidad y citación de perito.
2. Debe cumplirse con los requisitos generales para la admisibilidad de las solicitudes de prueba. En este punto es preciso referirse a la norma del artículo 259, inciso final, CPP, que dispone que, para comparecer al juicio oral, los peritos deben haber sido determinados por el fiscal en su acusación. Asimismo, el artículo 261 del CPP señala que, respecto del querellante, deberá incluir al perito en su escrito de adhesión a la acusación del Ministerio Público o acusación personal. Respecto del acusado, deberá señalar los peritos en su contestación a la acusación, como lo señala el artículo 263 letra c). Con todo, la ley señala casos excepcionales en que puede incorporarse la prueba en la forma que señala el artículo 296 CPP.
3. Debe el juez estimar que los peritos y sus informes otorgan suficientes garantías de seriedad y profesionalismo.
4. Es posible para el juez limitar el número de informes o de peritos, cuando unos y otros resultaren excesivos o pudieran entorpecer la realización del juicio.
5. Los honorarios y demás gastos derivados de la intervención de los peritos corresponderán a la parte que los presentare. A pesar de esto, el artículo permite que el juez releve a la parte del pago de remuneración del perito cuando considerare que ella

> no cuenta con medios suficientes para solventarlo o cuando tratándose del imputado, la no realización de la diligencia pudiere importar un notorio desequilibrio en sus posibilidades de defensa.

El **artículo 317** se refiere a la **incapacidad para ser perito**. Al respecto, dispone que no podrán desempeñar esta función las personas a quienes la ley reconociere la facultad de abstenerse de prestar declaración testimonial, conforme establece el artículo 358 del CPC[95]. Se trata por lo tanto de personas afectas por vínculos que afectan su independencia, tales como el parentesco, dependencia, amistad o enemistad.

Los peritos, de conformidad con el **artículo 318**, no pueden ser inhabilitados por lo que no se puede accionar en su contra aduciendo causales de implicancia o recusación ni tachas. Con todo, "durante la audiencia del juicio oral podrán dirigírseles preguntas orientadas a determinar su imparcialidad e idoneidad, así como el rigor técnico o científico de sus conclusiones. Las partes o el tribunal podrán requerir al perito información acerca de su remuneración y la adecuación de ésta a los montos usuales para el tipo de trabajo realizado".[96]

La declaración de peritos está regulada en el artículo 319 del CPP:

---

[95] Art. 358 (347). Son también inhábiles para declarar:

1°. El cónyuge y los parientes legítimos hasta el cuarto grado de consanguinidad y segundo de afinidad de la parte que los presenta como testigos;

2°. Los ascendientes, descendientes y hermanos ilegítimos, cuando haya reconocimiento del parentesco que produzca efectos civiles respecto de la parte que solicite su declaración;

3°. Los pupilos por sus guardadores y viceversa;

4°. Los criados domésticos o dependientes de la parte que los presente.

Se entenderá por dependiente, para los efectos de este artículo, el que preste habitualmente servicios retribuidos al que lo haya presentado por testigo, aunque no viva en su casa;

5°. Los trabajadores y labradores dependientes de la persona que exige su testimonio;

6°. Los que a juicio del tribunal carezcan de la imparcialidad necesaria para declarar por tener en el pleito interés directo o indirecto; y

7°. Los que tengan íntima amistad con la persona que los presenta o enemistad respecto de la persona contra quien declaren.

La amistad o enemistad deberán ser manifestadas por hechos graves que el tribunal calificará según las circunstancias.

Las inhabilidades que menciona este artículo no podrán hacerse valer cuando la parte a cuyo favor se hallan establecidas, presente como testigos a las mismas personas a quienes podrían aplicarse dichas tachas.

[96] Artículo 318 CPP.

1. La declaración de los peritos en la audiencia de juicio oral se regirá por las normas previstas en el **artículo 329** y, supletoriamente, por las establecidas para los testigos. El precepto indicado establece que:

    1.1. Los peritos deberán ser **interrogados personalmente**, no pudiendo ser dicha declaración sustituida por la lectura de registros en que constaren anteriores declaraciones o de otros documentos que las contuviera, salvo las **excepciones** establecidas en los artículo **331 y 332**, que se refieren, respectivamente, a la **reproducción de declaraciones anteriores** a la audiencia del juicio oral bajo determinados supuestos; y la **permisión de lectura** de partes del informe del perito que él elaboró, cuando fuere necesario para ayudar su memoria, demostrar o superar contradicciones o para solicitar las aclaraciones pertinentes. Esto es manifestación del principio de oralidad que informa el proceso penal.

    1.2. El juez presidente de la sala **deberá identificar al perito ordenándose que preste juramento** o promesa de decir la verdad.

    1.3. Los peritos **deberán exponer brevemente el contenido y las conclusiones de su informe,** y a continuación se autorizará que sean interrogados por las partes, teniendo en primer lugar la parte que haya ofrecido la prueba.

    1.4. Luego, dispone el Código, los miembros del tribunal podrán **formular preguntas al perito** con el fin de aclarar sus dichos.

    1.5. Puede autorizarse que, a solicitud de parte, **vuelva a ser interrogado** el perito que ya hubiere declarado.

    1.6. Antes de declarar, los peritos **no pueden comunicarse entre sí**, ni ver, oír ni ser informados de lo que ocurriere en la audiencia.

    1.7. El artículo 329 permite, también, que, de hallarse impedido de comparecer a declarar a la audiencia de juicio oral por motivo grave y difícil de superar, el perito podrá declarar a través de **videoconferencia** o cualquier otro medio tecnológico apto para su interrogatorio o contrainterrogatorio. Para ello, será necesario que se convoque una audiencia previa a la que deberá comparecer el

perito ante el tribunal con competencia en materia penal más cercano al lugar donde se encuentre.

Si el perito se negare a prestar declaración se le aplicará lo dispuesto para los testigos en el artículo 299, el cual a su vez se remite al artículo 33, que prevé que en este caso podrá decretarse el arresto del perito hasta el momento de la audiencia, por un máximo de 24 horas y, adicionalmente, además de aplicársele una multa de hasta 15 unidades tributarias mensuales.

El artículo 321 se refiere al perito en los auxiliares del Ministerio Público.

Es relevante referirse a **la responsabilidad penal que puede imputársele al perito**, regulada en el artículo 208 del CPP que señala que cometen delito de perjurio el testigo, perito o intérprete que ante un tribunal faltare a la verdad en su declaración, informe o traducción.

8. Prueba directa y prueba indirecta.

Sabemos que la prueba es, en sentido estricto, "la verificación o confirmación de las afirmaciones de hecho expresadas por las partes".[97] Es de nuestro interés la distinción entre prueba directa y prueba indirecta, que puede fundarse en tres criterios:[98]

1. **Mediatez o inmediatez**: El primer criterio se refiere a sí el carácter de la prueba es mediato o inmediato, en el sentido de si coincide o no el hecho que se prueba con el que el juez percibe. De esta manera, la prueba directa es aquella en que la observación que el juez hace del hecho mismo que se prueba. Por su parte, prueba indirecta es "el procedimiento probatorio que permite llegar al hecho que se prueba a partir de otro u otros mediante un proceso inferencial".[99]
2. **Inferencia necesaria o probable:** Según este criterio una prueba es directa cuando en la inferencia aplican leyes lógicas y científicas para llegar a resultados necesarios. De contrario, sería prueba indirecta aquella en que en la inferencia se aplican "leyes

[97] OVALLE FAVELA, JOSÉ (2016) *Teoría General del Proceso.* 7ma Edición, Ciudad de México: Oxford University Press, p. 332.

[98] GASCÓN ABELLÁN, MARINA (2010) *Los hechos en el derecho. Bases argumentales de la prueba.* Tercera edición. Madrid: Marcial Pons, p. 79.

[99] Ibid.

probabilísticas", como las máximas de la experiencia, que solo conducen a resultados probables o posibles.[100]

3. **Necesidad de raciocinio.** Este es el tercer criterio, y es el que prevalece en la doctrina y jurisprudencia, en donde la prueba directa es, básicamente, aquella en que el hecho que "se quiere probar aparece directa y espontáneamente, sin mediación alguna ni necesidad de raciocinio y que es capaz por si sola de fundar la convicción del tribunal".[101] Mientras que la prueba indirecta es aquella en que el hecho que se quiere probar no surge directamente del medio de prueba, sino que requiere de raciocinio y es "incapaz por si sola de fundar la convicción judicial sobre ese hecho".[102] Ejemplos de prueba directa serían la testimonial y documental.[103]

No obstante, es difícil establecer esta distinción en términos absolutos o sin entrelazar los diversos criterios. No toda prueba se subsume por completo dentro de una u otra categoría. Para efectos de nuestra investigación, hemos entendido que la prueba es directa o indirecta a la luz del primer criterio, esto es, si es inmediata o mediata.

De su parte, **Taruffo** hace una distinción entre **prueba real y prueba circunstancial,** siendo las primeras aquellas que "consisten en sucesos, comportamientos, situaciones u objetos que son o pueden ser directamente percibidos por el juzgador".[104] Por ejemplo, material audiovisual, la inspección personal del tribunal, etc. Las **pruebas circunstanciales,** en cambio, son aquellas en que "las inferencias acerca de la verdad de un enunciado sobre un hecho principal se obtienen asumiendo otro hecho como premisa", y a este se le considera "un medio de prueba indirecto sobre aquel hecho principal".[105] De esta manera, cualquier circunstancia o hecho tendrá valor

[100] Ibid., p. 80.

[101] Ibid.

[102] Ibid.

[103] Ibid.

[104] TARUFFO, MICHELE (2008) *La prueba.* Madrid: Marcial Pons, p.102.

[105] Ibid., p. 104.

probatorio mientras a partir de este el juez pueda "obtener conclusiones inferenciales sobre la verdad o falsedad de un hecho en disputa"[106]

9. La prueba mediante presunciones.

a. Generalidades.

Como ya señalamos antes, la prueba mediante geolocalización constituye un indicio de la participación de un delito, puesto que **no acredita directamente** su perpetración ni la participación de nadie en él, sino que permite al juez inferir aquello, a través de una presunción.

La doctrina clásica chilena define presunción como "el resultado de una operación lógica, mediante la cual partiendo de un hecho conocido se llega a aceptar como existente otro hecho desconocido o incierto".[107]

Al respecto, **Casarino**, con su clarísima pluma, nos indica que la prueba por presunciones consta de "diversos elementos que lo integran, a saber: los antecedentes o circunstancias conocidos, que reciben el nombre de indicios o bases, en atención a que sobre ellos se construye la o las presunciones; la operación de raciocinio lógico del legislador o juez que, partiendo del indicio o base anterior, llega al establecimiento del hecho desconocido y controvertido; y, en fin, el hecho desconocido y controvertido mismo, el cual, una vez operada la presunción, deja de ser tal para convertirse en su objeto.[108]

Ahora bien, existen **presunciones legales y judiciales**. Las primeras las establece la ley y las segundas, el juez. Esta últimas consisten en "un mecanismo propio del juzgador mediante el cual por deducción o inducción se llega al conocimiento de un hecho primeramente

---

[106] Ibid., p. 105.

[107] ALESSANDRI, A.; SOMARRIVA, M. & VODANOVIC, A. (1998) *Tratado de Derecho Civil.* Tomo II. Santiago de Chile: Editorial Jurídica de Chile, p. 485.

[108] CASARINO, MARIO (1984) *Manual de Derecho Procesal.* Tomo IV. Cuarta Edición. Santiago de Chile: Editorial Jurídica de Chile, p. 201.

desconocido, partiendo de la existencia de un hecho conocido".[109] Y son estas las que interesan al propósito de nuestra investigación y, particularmente, las del proceso penal.

En materia civil, el código del ramo establece en su artículo 1712 que las presunciones judiciales deben ser graves, precisas y concordantes. Graves "porque fuerza es que el hecho conocido en que se apoya la presunción haga sacar la consecuencia casi necesaria del hecho desconocido que se busca; precisas porque la presunción no debe ser vaga ni capaz de aplicarse a muchas circunstancias; concordantes, pues las presunciones no deben destruirse las unas a las otras".[110]

Pero, en materia penal en la actualidad no existe regulación alguna. La justificación de esto sería que "los indicios o presunciones judiciales deben ser construidos por el tribunal sin que se establezcan parámetros para ello por parte del legislador, al regir el sistema de la sana crítica como sistema probatorio".[111]

Con anterioridad, el Antiguo Código de Procedimiento Penal regulaba las presunciones judiciales en su artículo 488, requiriendo que (1) se fundaran en hechos reales y probados y no en otras presunciones; (2) fueran múltiples y graves; (3) fueran precisas; (4) fueran directas; y (5) concordantes. No obstante que el actual Código Procesal Penal no regule las presunciones judiciales, sino que se admite su procedencia en virtud de la regla de libertad probatoria consagrada en el artículo 295 del mismo. Por consiguiente, no se presentan requisitos para su admisibilidad. Sin embargo, la jurisprudencia exige, como vimos en el capítulo precedente, la concurrencia de requisitos respecto de los indicios en que se basa la presunción judicial. Además, como se verá en el capítulo siguiente, la presunción debe estar debidamente fundada por el tribunal.

b. Elementos de la presunción.

La doctrina establece tres elementos de toda presunción:

---

[109] GÓMEZ LARA, CIPRIANO (2012) *Teoría general del proceso.* Décima edición. D.F. de México: Oxford University press, p. 314.

[110] ESCRICHE, Citado en Ibid., pp. 485-486.

[111] MATURANA & MONTERO op. cit. p. 860.

1. **Hecho conocido**, que es la base de la presunción; y que deberá estar plenamente probado en el proceso.
2. **Elemento lógico o actividad racional** respecto del hecho conocido, para unirlo con el hecho desconocido.
3. **Hecho presumido,** que era desconocido pero que es posible inferir a partir de los dos elementos anteriores.[112]

c. Presunción puesta en práctica.

Aterrizando estos conceptos a la técnica de geolocalización, la presunción permitirá que, a través de la correcta operación lógica del juez, puesta tener por cierto un hecho desconocido, a saber, la participación del sospechoso en la comisión del delito, a partir del hecho conocido (indicio) de que se encontraba en un área cercana al sitio del suceso, a partir del análisis del perito de los archivos que emanaron del sistema de geolocalización asociado a la telefonía celular.

10. Indicios.

a. Generalidades.

La palabra indicio proviene del latín indicium, que es una derivación de indicere, cuyo significado es indicar, hacer, conocer algo.[113] Consistente con lo anterior, la prueba indiciaria es aquella en que, a partir de hechos conocidos, deduce otros que se desconocen, sobre ellos, a su vez, se construirá una presunción. Así, el indicio es también llamado **hecho base, o hecho indicador**. Por la otra parte tenemos el **hecho presumido, hecho consecuencia o hecho indicado**, indistintamente.

El indicio permite, a través de una inducción o una deducción lógica, la inferencia de un o unos hechos desconocidos o que no han sido probados, a partir de un o unos hechos conocidos y debidamente probados. Por consiguiente, el indicio es el "medio de confirmación indirecto que

[112] MATURANA & MONTERO, Óp. Cit. pp. 857-858.

[113] ALVARADO VELLOSO, ADOLFO (2009) *Sistema procesal*, Santa Fe, Argentina: Rubinzal-Culzoni editores, p. 66.

le permite al juez obtener el resultado de una presunción que, a su turno, es el juicio lógico que permite al juzgador tener como cierto o probable un hecho incierto después de razonar a partir de otro hecho cierto".[114]

Existen además los indicios **necesarios y los contingentes.** Indicio necesario es aquel que se vale por sí solo para inferir un hecho presumido. Contingente en cambio, es aquel que requiere de otros indicios para que el juez realice tal inferencia.[115]

Hay autores, como el argentino Adolfo **Alvarado Velloso**, que establecen requisitos de existencia, de validez y de eficacia para los indicios.

Requisitos de existencia de los indicios:

1. Indicio plenamente probado.
2. Que tal indicio "tenga alguna significación confirmatoria respecto del hecho que genera el razonamiento indiciario, por existir alguna conexión lógica entre ellos".[116]

Requisitos de validez de los indicios:

1. Que el medio que prueba el indicio haya sido decretado y practicado de acuerdo con la ley, por medios lícitos y no prohibidos.
2. Que no exista una causa general de nulidad del proceso que vicie el indicio.
3. Que no esté prohibida la investigación del hecho base ni hecho consecuencia.[117]

Requisitos de eficacia de los indicios:

1. Conducencia del medio indiciario con respecto al hecho investigado.

[114] Ibid., pp. 66-67.

[115] Ibid., p. 67.

[116] Ibid., pp. 98 – 99.

[117] Ibid., 99 -100.

2. Que se haya descartado que la relación entre hecho base y hecho consecuencia es obra de la casualidad o del azar, como también posibilidad de falsificación del indicio.
3. Que exista una clara y cierta relación de causalidad entre hecho base y hecho consecuencias.
4. Que sean varios, graves, precisos y concordantes cuando se trate de indicios contingentes.
5. Que no haya contraindicios difíciles de descartar razonablemente.
6. Que las hipótesis alternativas hayan sido eliminadas.
7. Que el resultado sea unívoco e inequívoco.
8. Que no existan medios de prueba que contradigan los indicios o planteen un hecho opuesto a ellos.
9. Que se llegue a una conclusión precisa y segura a través del pleno convencimiento del juez.

Sin perjuicio de estas extensas apreciaciones doctrinales, para resolución de casos de mediana dificultad, basta con comprender que el **hecho base debe estar plenamente probado** en el proceso. Y, por otra parte, debe expresarse con claridad por el Tribunal el raciocinio o reflexión lógica que le permite engarzar el hecho base con el hecho consecuencia; es decir, debe estar motivado. Como se verá más adelante.

Indicios en la Jurisprudencia chilena.

La Corte de Apelaciones de Concepción, en septiembre de 2019, pronunciándose acerca un recurso de nulidad de una sentencia penal condenatoria declaró que (1) los hechos deben estar plenamente probados; (2) "que los hechos constitutivos del delito o participación se deduzcan de los primeros, a través de un proceso mental razonado y acorde con las reglas del criterio humano". "Y si los hechos probados permiten diversas conclusiones o interpretaciones, (3) que la sentencia explique su elección".[118]

[118] CORTE DE APELACIONES DE CONCEPCIÓN (2019) *Sentencia de 17 de septiembre de 2019, ROL 731-2019.* Considerando 7°.

Citando un fallo de la Corte Suprema, la Corte de Apelaciones declara que "el nexo entre el hecho base y el hecho consecuencia deber ser coherente, lógico y racional. Su falta de concordancia con las reglas del criterio humano, que pueden tener su origen en la falta de lógica o de coherencia en la inferencia como por el carácter excesivamente abierto, débil o indeterminado de la misma, harán que las presunciones sean inaptas para lograr la convicción necesaria para hacer desaparecer la presunción de inocencia del imputado y, en definitiva, establecer su culpabilidad".[119]

Según la Ilustrísima Corte, los indicios abiertos, débiles y equívocos no permiten excluir hipótesis alternativas, menos cuando no son vinculadas de manera coherente, lógica y racional con los hechos consecuencia; siendo insuficientes los razonamientos de este tipo. Por estas razones se falló en favor de la nulidad de la condena en este caso en particular.[120]

En definitiva, para que el tribunal presuma la comisión de un delito o la participación de un imputado en ella, será necesario que el hecho base se encuentre debidamente probado, y que el indicio sea coherente, lógico y racional. Esto último dice relación con la sana crítica como sistema de valoración de la prueba, establecido en el artículo 297 del CPP, en especial con los principios de la lógica y las máximas de experiencia como indispensables para enervar el principio de presunción de inocencia y superar el estándar de convicción más allá de toda duda razonable.

En nuestro caso particular, estimamos que la técnica de geolocalización propuesta dará pie a un fuerte indicio de la participación de sospechosos en la comisión del delito.

11. Valoración de la prueba.

a. Generalidades.

La valoración de los medios de prueba es una de las vertientes del derecho a la prueba. Se la ha definido como "el derecho que tienen las partes a que, al momento de emitir sentencia, el juez

[119] CORTE SUPREMA (2005) *Rol N° 740-2005*, citada en ibid.

[120] Op. Cit. nota 75, considerando 8°.

analice los medios de prueba que han sido actuados en el proceso".[121] Asimismo, se ha dicho que la **valoración de la prueba consiste** en un "complejo proceso que implica determinar qué conclusiones se pueden obtener de aquellos medios que han sido actuados en el proceso respecto de los hechos controvertidos".[122] Esta tiene por objeto "establecer la conexión final entre los medios de prueba presentados y la verdad o falsedad de los enunciados sobre los hechos en el litigio".[123]

La valoración de la prueba se desarrolla en las siguientes **etapas**: (1) identificación, por el juez, de los medios que se refieren a los hechos controvertidos; (2) valoración individual de las evidencias teniendo en vista los hechos controvertidos; (3) comparación de las consecuencias obtenidas de cada evidencia para establecer "conclusiones que sean coherentes entre sí", de forma de obtener la hipótesis más probable; y (4) juicio lógico inferencial del juez a partir de la valoración conjunta de los medios de prueba.[124]

Concluyentemente, **los resultados de la valoración** podrán ser que (1) lo más probable es que haya ocurrido el hecho; (2) que no haya ocurrido el hecho; y (3) que no sea posible concluir la ocurrencia o no de un hecho.[125]

b. Sistemas de valoración de la prueba.

Existen, en general, dos sistemas probatorios; a saber, el sistema de valoración legal, y el sistema de valoración judicial. El primero tiene carácter apriorístico y extrajudicial; y el segundo es a posteriori y se subdivide en el sistema de la libre convicción y el sistema de la sana crítica.

b.1. Sistema de libre o íntima convicción.

Maturana y **Montero** señalan que "en materia probatoria, libre es el juez que puede dar o no dar por probados los hechos, cualesquiera que sean las pruebas que haya en el proceso. Este juez

---

[121] PRIORI POSADA, GIOVANNI (2019) *El proceso y la tutela de los derechos.* Lima: Pontificia Universidad Católica del Perú, Fondo Editorial, p. 109.

[122] Ibid. p.110.

[123] TARUFFO (2008) Op. Cit., p. 132.

[124] Ibid., pp. 109 -110.

[125] Ibid. p. 111.

no está sometido a medios, procedimientos ni reglas de valoración".[126] Este sistema supone una forma de **convencimiento libre por parte del juez**, como puede ser el "conocimiento intuitivo; prueba hallada fuera autos; saber privado del juez respecto de los hechos que debe apreciar".[127]

En definitiva, las **características fundamentales** de este sistema son (1) la libertad absoluta que tiene el juez para valorar la prueba; y (2) el juez no está en obligación de fundamentar su fallo [prescindencia del principio de socialización de la sentencia];

No obstante, se crítica este sistema debido a que se puede fallar la causa por la "apreciación afectiva y/o subjetiva de los hechos", puesto que no requiere ni siquiera de motivación[128]. En otras palabras, estaría fallando de manera irracional, incontrolable y arbitraria.[129] Así también, y como consecuencia de la falta de motivación, se reprocha la dificultad para controlar un tribunal superior el mérito del fallo.[130] Se sostiene que el juez "no puede ser libre de no observar una metodología racional en la fijación de hechos controvertidos".[131]

b.2. Sistema de la prueba legal o tasada.

Se trata del opuesto al sistema anterior, toda vez que se basa en "la aplicación de reglas legales establecidas a priori" y en el "valor probatorio de algunos tipos de medios de prueba", de manera que los jueces tengan que valorizar la prueba según dichas reglas preestablecidas.[132] Se originó para poner límite a las arbitrariedades de los jueces en que predominaba el principio inquisitivo.

Con este sistema se aspira no ya a la verdad suficiente, sino que la "certeza histórica legal respecto de los hechos".[133] El juez tiene el papel de aplicador de la norma jurídica que valoriza la prueba.

Por esto último este sistema ha sido criticado, toda vez que deja nula discreción al juez.

---

[126] MATURANA & MONTERO (2010) Op. Cit. p. 918.

[127] Ibid.

[128] Ibid. p. 919.

[129] Ibid. p. 920.

[130] Ibid. p. 219.

[131] Ibid. p. 920.

[132] TARUFFO (2008) Op. Cit. p. 133.

[133] MATURANA & MONTERO (2010) Op. Cit. p. 921.

Se le critica también por no encaminar a una comprobación racional de la verdad de los hechos, sino sólo hacia la "certeza puramente formal".[134]

Un ejemplo de este sistema tasado, aunque morigerado, lo tenemos en nuestro Código de Procedimiento Civil.

b. 3. Sistema de la sana crítica.

La arbitrariedad que supone la libre convicción, y, por el otro lado, la rigidez de la prueba tasada, condujeron a que se desarrollara una tercera vía, que evitase ambos extremos.

La sana crítica se encuentra dentro del sistema de libre valoración de la prueba, pero no permite que el juez llegue a la convicción de manera subjetiva y arbitraria, sino que utilizando razonablemente la lógica y la experiencia.[135]

Couture sostiene que "la sana crítica está integrada por reglas del correcto entendimiento humano, contingentes y variables, con relación a la experiencia del tiempo y lugar, pero que son estables y permanentes en cuanto a los principios lógicos en que debe apoyarse".[136]

Maturana y **Montero** extraen de esta cita dos principios del sistema de la sana crítica, a saber, que (1) el juez "debe actuar de acuerdo a las reglas de la lógica"; y (2) que debe actuar aplicando las reglas de la experiencia, que sería el "conjunto de juicios fundados sobre la observación de la experiencia que ocurre comúnmente y que pueden formularse en abstracto por toda persona de nivel mental medio".[137] Adicionalmente, habría que agregar como tercera limitación a la libre apreciación los conocimientos científicamente afianzados.

En cuanto a la experiencia, el juez la obtiene "de la labor que ejerce y el medio social en que se desenvuelve y varía según el tiempo, lugar y medio social en que se desarrolla la labor de éste".[138]

---

[134] Ibid.

[135] Ibid. p. 922.

[136] Couture; Citado en: ibid. p. 922.

[137] STEIN; Citado en: ibid.

[138] Ibid.

En contraposición a las máximas de la experiencia, las reglas de la lógica tienen el carácter de "universales, estables e invariables en el espacio y el tiempo".[139]

Como consecuencia de esta libertad de apreciación, para prevenir la arbitrariedad, se tiene el deber de fundamentación del juez, de forma que se permita repetir mentalmente la valoración de las pruebas y el razonamiento que lo condujo a fallar en un sentido u otro.[140]Es por ello que la sana crítica tiene una relación directa con la motivación de las sentencias. Incluso con anterioridad a la entrada en vigor del CPP, en doctrina **Alessandri** sostuvo que "debe puntualizarse en la sentencia la operación lógica que lo llevó [al juez] al convencimiento".[141]

Taruffo sostiene que "los procesos psicológicos del juez, sus reacciones íntimas y sus estados individuales de conciencia no le interesan a nadie: lo que interesa es que se justifique su decisión con buenos argumentos".[142] En este sentido, la sana crítica es vista como contralora de los fundamentos de la sentencia, toda vez que ella "debe aparecer como una operación racional, motivada en elementos de prueba legítimos", que serían los razonamientos hechos a partir de las reglas de la lógica y las máximas de la experiencia.[143]

c. Valoración de la prueba en el proceso penal chileno.

En el proceso penal chileno, el sistema de valoración de prueba utilizado es el de la sana crítica. Si bien no lo señala expresamente, se deduce a partir de las limitaciones que impone al juez.

En efecto, el inciso primero del artículo 297 del CPP prescribe lo siguiente: "Los tribunales apreciarán la prueba con libertad, pero no podrán contradecir los principios de la lógica, las máximas de la experiencia y los conocimientos científicamente afianzados".

Entonces, si bien existe libertad en la valoración, ella no es absoluta, sino que deben respetarse los principios de la lógica, las máximas de la experiencia y los conocimientos científicamente afianzados.

---

[139] Ibid. p. 923.

[140] Ibid. p. 927.

[141] ALESSANDRI et al. (1998) op. cit. p. 487.

[142] TARUFFO, citado en: MATURANA & MONTERO (2010) Op. Cit. p 931.

[143] Ibid. p. 929.

A continuación, el artículo 297 al regular la obligación fundamentar la prueba establece que "[e]l tribunal deberá hacerse cargo en su fundamentación de toda prueba producida, incluso de aquella que hubiere desestimado, indicando en tal caso las razones que hubiere tenido en cuenta para hacerlo."

La valoración de la prueba en la sentencia requerirá el señalamiento del o de los medios de prueba mediante los cuales se dieren por acreditados cada uno de los hechos y circunstancias que se dieren por probados, de forma tal que sea factible la reproducción del razonamiento utilizado para alcanzar las conclusiones a que se arribó en la sentencia.

Por su parte, el inciso final busca garantizar la socialización de la sentencia, de forma tal que cualquier persona pueda recrear el razonamiento del tribunal. Es así como este inciso dispone lo siguiente: "La valoración de la prueba en la sentencia requerirá el señalamiento del o de los medios de prueba mediante los cuales se dieren por acreditados cada uno de los hechos y circunstancias que se dieren por probados. Esta fundamentación deberá permitir la reproducción del razonamiento utilizado para alcanzar las conclusiones a que llegare la sentencia."

Adicionalmente, otros artículos que se refieren la materia, es el caso de las letras c) y d) del artículo 342 donde se indica que la sentencia debe exponer de manera clara, lógica y completa los hechos probados y la valoración de los medios de prueba en que se basen; y "las razones legales o doctrinales que sirvieren para calificar jurídicamente cada uno de los hechos y sus circunstancias y para fundar el fallo".[144]

12. Estándar de la prueba.

a. Generalidades.

Los estándares probatorios pueden entenderse como aquellos que "determinan cuándo resulta justificado aceptar (o rechazar) una proposición fáctica en un proceso judicial, a pesar de las condiciones de incertidumbre en las que ese juicio tiene lugar".[145]

[144] 342 CPP.

[145] ACCATINO, DANIELA (2011) *Certezas, dudas y propuestas en torno al estándar de la prueba penal.* Revista de Derecho de la Pontificia Universidad Católica de Valparaíso XXXVII [pp-483-511] p.486.

Daniela **Accatino** toma de Jordi **Ferrer** la distinción entre "diversos momentos de la actividad probatoria"[146]: el primer momento, también llamado **valoración en sentido estricto**; y el segundo, al que denomina momento de **decisión sobre la prueba.**

El **primer momento** consiste en determinar o corroborar si existe o no una relación entre las evidencias y "los hechos del caso que son objeto del proceso" [147], basándose en los conocimientos científicamente afianzados y en las máximas de la experiencia, de forma que las evidencias sirvan como inducciones probabilísticas más que demostraciones de la verdad de una hipótesis. Este primer momento tiene por finalidad confirmar si la hipótesis sirve como una "explicación posible de la existencia de las evidencias valoradas" [148] En efecto, este primer momento, al que ya nos referimos en el título anterior, tendrá por resultado la "individualización de las pruebas […] y la identificación de factores que inciden en su mayor o menor fuerza probatoria"[149], por razones de credibilidad o autenticidad, su carácter de prueba directa o indirecta; también es este el momento en que se excluye la prueba irrelevante o defectuosa.

El **segundo momento, de decisión sobre la prueba** viene a despejar si las evidencias, que hasta este punto solo corroboran medianamente la verdad de una hipótesis, son suficientes para tener por probada dicha hipótesis. **Acattino** al respecto, señala que "[p]recisar cuál es el nivel de suficiencia requerido en un determinado procedimiento es, precisamente, la tarea propia de los estándares de prueba".[150]

En nuestro caso, el primer momento corresponde a la corroboración de que la comisión del delito sirve como explicación de la existencia de llamadas efectuadas por el sospechoso, registradas en el C.D.R de una antena o estación base que cubre el área del sitio del suceso. En otras palabras, analizar si existe cierta probabilidad de que haya una relación entre las evidencias y la hipótesis planteada, que supere la incertidumbre y sea reconocido como un medio de prueba dentro del proceso, usando como herramienta para dilucidar este asunto los conocimientos científicamente afianzados y las máximas de la experiencia. A continuación, en el segundo

[146] ACCATINO (2011). p. 484 nota al pie de página N°3.

[147] Ibid. 485.

[148] Ibid.

[149] Ibid.

[150] Ibid. p. 486.

momento, correspondería establecer si dicha geolocalización es suficiente para dar por cierta la hipótesis del caso, a saber, que el sospechoso tuvo participación en los hechos.

Existen diversos estándares probatorios, según cuál sea su nivel de exigencia. Así existe el llamado estándar mínimo o de **preponderancia de la prueba,** mediante el cual se tendrá por probado el hecho o proposición fáctica que sea más corroborado por las evidencias disponibles, de manera que se descarten las otras por tener menor cantidad de pruebas a su favor.[151] Este estándar es el utilizado en los procesos civiles.

En cambio, existen otros estándares más exigentes, que reducen el riesgo de tener por verdadero un hecho o proposición fáctica que en realidad es falso, puesto que se requerirá de una prueba de mayor magnitud para darlo por acreditado, y no basta con la preponderancia relativa a la que nos referimos en el párrafo anterior.

Martina **Cociña** ha sostenido que "la determinación del estándar es una decisión netamente política, que remite directamente al nivel probatorio exigido en el proceso punitivo, y específicamente, a la discusión de cuantas absoluciones falsas se van a permitir como sociedad, con tal de impedir una condena errónea. Por este marcado carácter político que conlleva el grado de prueba, se afirma adecuadamente que el estándar probatorio en el ámbito penal constituye la voz de la ideología político-criminal que acoge una determinada nación".[152]

De esta forma, como sociedad se prefiere el error negativo al error positivo. Es decir, es más aceptable absolver a una persona responsable que condenar a una persona inocente. A partir de este razonamiento se formula principio de inocencia.

b. Estándar de la probabilidad prevalente.

En definitiva, el estándar de probabilidad prevalente "implica tanto que la pretensión del demandante debe ser más probable que su negación, como que, ante diversas hipótesis, el juez debe elegir aquella que disponga de un mayor grado de confirmación relativa".[153]

---

[151] Ibid.

[152] COCIÑA, MARTINA (2012) *La verdad como finalidad del proceso penal.* Santiago de Chile: Thomson Reuters, p. 103.

[153] MATURANA & MONTERO (2017) Op. Cit. p 80.

Existen entonces dos reglas que operan en este sistema, a saber, (1) la regla de "más probable que no"; y (2) la de "prevalencia relativa de la probabilidad".

La primera regla consiste en que cuando, a partir de la prueba rendida, la veracidad del hecho sea más probable que su falsedad entonces se le debe tener por cierto. Mientras que la regla de la prevalencia relativa de la probabilidad consiste en que cuando hay una multiplicidad de hipótesis sobre los hechos, prevalecerá aquella que se demuestre predominante frente a las otras. Una vez resuelto esto, corresponde aplicar la primera regla; es decir, si es más probable la veracidad de la hipótesis que su falsedad.

En el proceso civil se exige que "ninguna prueba sea admitida si su probabilidad no sobrepasa el 50%"; [154] lo que se conoce como primacía de la prueba. De esta forma prevalece la hipótesis más convincente, sea la del demandante o la del demandado. Ahora bien, en casos en que se ve afectada la libertad individual, existe la regla de la prueba clara y convincente, donde se exige un nivel de 60 a 65% de probabilidad; por ejemplo, en caso de internamiento psiquiátrico.[155]

c. Estándar de convicción más allá de toda duda razonable.

En materia penal, el artículo 340 del Código Procesal Penal establece el estándar probatorio en los siguientes términos: "Nadie podrá ser condenado por delito sino cuando el tribunal que lo juzgare adquiriere, **más allá de toda duda razonable,** la convicción de que realmente se hubiere cometido el hecho punible objeto de la acusación y que en el hubiere correspondido al acusado una participación culpable y penada por la ley.

El tribunal formará su convicción sobre la base de la prueba producida durante el juicio oral."

Como podemos apreciar, el legislador se decantó por el estándar de prueba de la convicción más allá de toda razonable, sin embargo, no especifica ni entra en detalles sobre qué debe entenderse por tal.

[154] MATURANA & MONTERO (2010) p. 940.

[155] Ibid.

Al respecto, se señala que este criterio proviene del desarrollo del derecho anglosajón, en donde se le conoce como *beyond a reasonable doubt*, y se aplica en el sistema penal, a diferencia de su sistema civil que establece el criterio de preponderancia de la prueba.

Se trata de una "noción genérica, que independiente de las tentativas que se efectúen por delimitarlo, siempre permanecerá un espacio de incertidumbre que no permitirá obtener una idea clara sobre lo que realmente implica."[156] De hecho, en el sistema del *common law*, ha sido entendido de múltiples maneras por los distintos jueces: (1) "como la seguridad de creencia apropiada para las decisiones importantes de la vida de uno"[157]; (2) "como el tipo de duda que haría vacilar a una persona prudente de actuar o no"[158]; (3) "como una convicción perdurable de culpabilidad"[159] ; (4) "la duda razonable como la duda por la cual se puede dar una razón"[160]; y (5) "como probabilidad alta"[161]. Sin perjuicio de que algunas de tales nociones fueron posteriormente desconocidas por los tribunales superiores estadounidenses.[162]

Todos estos significados han sido desarrollados por los jueces para efectos de orientar al jurado a la hora de decidir si el acusado(a) es o no culpable.

Finalmente, el problema producido por el hecho de que tales definiciones no fueran "diferentes interpretaciones de una misma noción sino diferentes concepciones acerca del nivel de prueba necesario para condenar a una persona por un delito"[163], junto con la contradicción que existía al respecto entre los tribunales de justicia, "ha provocado que muchas cortes de apelación indiquen a los tribunales de juicio que no deben dar definiciones del 'más allá de toda duda razonable' en sus instrucciones a los miembros del jurado"[164].

---

[156] COCIÑA (2012) Op. Cit. p. 103.

[157] LAUDAN, LARRY (2011) *El estándar de prueba y las garantías en el proceso penal.* Buenos Aires: Hammurabi, p. 131.

[158] Ibid. P, 133.

[159] Ibid. P, 137.

[160] Ibid. P. 141.

[161] Ibid. P. 150.

[162] Ibid. P. 131.

[163] Ibid. P. 157.

[164] Ibid.

En otro contexto se ha entendido la duda razonable como aquella "que llevaría a las personas prudentes a dudar antes de actuar en materias importantes para ellos mismos. Es una duda basada en evidencia o falta de evidencia"[165]. Desde esta perspectiva, se estima que se satisface el criterio de más allá de toda duda razonable "si hay, entre otros requisitos, credibilidad, firmeza a lo largo del procedimiento y corroboración mediante datos objetivos"[166], y, de contrario, "Si existieren fundadas incertidumbres sobre la culpabilidad o la participación, el tribunal deberá absolver al acusado."[167]

En síntesis, la conceptualización de la convicción más allá de toda duda razonable podría construirse a partir de dos principios:

1. Vacilación para actuar o *hesitate to act*: proveniente de la jurisprudencia de la Corte Suprema norteamericana, en donde se le define como "la clase de duda que haría a una persona vacilar antes que actuar."[168] Sin embargo, se ha criticado esta aproximación por subjetivar asuntos que son de orden público, dejándolo en manos de cada individuo.
2. Certeza moral: Identifica el estándar con "la firme convicción de encontrarse en posesión de la verdad."[169] La certeza moral diferencia de la certeza absoluta, propia, cuya precisión matemática es imposible de utilizar en juicio penal. La certeza moral "consiste en el nivel más alto de convicción que se puede alcanzar en un juicio penal."[170] Si bien este es el criterio que se ha preferido por el ordenamiento jurídico chileno, no está exento de críticas.

En palabras de Daniela **Accatino**, en Chile se optó por adoptar el estándar de "más allá de toda duda razonable" teniendo en consideración la "ventaja de explicitar que una hipótesis que deba tenerse por probada puede, sin embargo, merecer algún grado de dudas".[171] El problema,

---

[165] MATURANA, CRISTIÁN (2006) *Aspectos generales de la prueba,* apuntes de clases, Escuela de Derecho, Universidad de Chile, p.29.

[166] COCIÑA. Op. Cit. p. 106.

[167] Íbid.

[168] NARANJO E IBARROLA ABOGADOS (2019) *Aspectos Generales de la Prueba: basado en la separata de Maturana 2015,* p. 44.

[169] Ibid.

[170] Ibid.

[171] ACCATINO (2011) Op. cit.p.493.

sostiene la autora, radica en decantar lo que se debe entender por suficiente para que el juez tenga por probadas las proposiciones fácticas, asunto que aún es controversial. Además, en Chile esta tarea se vuelve todavía más ardua, por cuanto se le exige al tribunal justificar con detalle sus decisiones acerca de la prueba, obligación que no existe en el sistema anglosajón.[172]

Otro inconveniente que se produce, según **Accatino**, es el que se refiere al "peligro de una lectura subjetivista" del precepto en cuestión, al cual se ha referido Julián **López**, quien sostiene que para superarlo se debe recurrir a la noción de certeza moral, cuyo entendimiento ya existía entre los jueces del antiguo proceso penal, a partir del artículo 456bis del antiguo Código de Procedimiento Penal que consagraba la certeza moral absolutoria, a partir de la cual era posible, a pesar de existir certeza legal condenatoria (plena prueba en virtud de reglas legales de valoración de esta), absolver al acusado cuando no hubiera un convencimiento a nivel subjetivo del juzgador respecto de la verosimilitud de los hechos. Este autor concibe la certeza moral en este mismo sentido.[173] No obstante, para **Accatino** resulta "difícil comprender qué ventajas"[174] podría traer esta concepción en un sistema de libre valoración de la prueba como el vigente hoy.

Finalmente, en el texto en análisis, Daniela **Accatino** recomienda evitar la subjetividad al momento de estimar si hay o no convicción más allá de toda duda razonable, de forma que la "duda no se presente de hecho en el ánimo del juzgador, sino que la duda haya debido suscitarse a la luz de las evidencias disponibles" [175], es decir, que se funde sobre pruebas que presentan defectos. En consecuencia, nadie podría ser condenado si las pruebas disponibles dan origen a dudas en cuanto a los hechos acaecidos o a la participación del acusado en ellos. A continuación, vendría la tarea de establecer "qué condiciones deben ser superadas por las pruebas disponibles para que pueda ser justificado tener por probada la versión de los hechos de la acusación"[176], que consistiría en distinguir las dudas irrelevantes de las "dudas justificadas en las pruebas disponibles"[177]. Para esta autora, debe considerarse como un defecto en las pruebas disponibles,

[172] Ibid. p. 494.

[173] Ibid. p. 495.

[174] Ibid. p. 496.

[175] Ibid. p. 503.

[176] Ibid. p. 504.

[177] Ibid.

aquellos que afectan a la prueba de forma tal que "no logren eliminar o refutar alguna proposición fáctica alternativa plausible y compatible con la inocencia del imputado".[178]

En lo que nos interesa, el peritaje a partir del cual se localiza la ubicación de determinados sospechosos en un área cercana al sitio del suceso no es por sí misma una prueba que supere el estándar de convicción más allá de toda duda razonable; no sería suficiente para condenar a un sospechoso, de forma tal que, si fuera la única prueba, debiera absolverse, en virtud del principio de presunción de inocencia e *in dubio pro reo*. No obstante, sí puede ser un indicio importante que, en conjunto con otras pruebas, permitiría obtener dicha certeza. Por ejemplo, que se presenten registros audiovisuales de los sospechosos, presencia de su ADN en el sitio del suceso, etc.

[178] Ibid. p. 507.

Capítulo III: Datos de tráfico de telecomunicaciones y Derechos Fundamentales.

En este capítulo analizaremos de qué manera el respeto a las garantías fundamentales modela la forma como será legítimo (o no) desarrollar actividades de tratamiento de datos de tráfico de telecomunicaciones en el marco de una investigación penal. Al respecto, debemos tener a la vista que estos daos podrían tener el carácter de dato personal, en los términos de la letra f) del artículo 2° de la ley 19.628, y lo previsto en el artículo 19 N° 4 de la Constitución Política de la República. Adicionalmente, podrían verse afectado el derecho al secreto de las comunicaciones, consagrado en el artículo 19 N° 5 de la Constitución Vigente.

A estas garantías específicas debemos sumar lo que señalamos antes respecto de la garantía del debido proceso legal.

1. Protección de la Privacidad y protección de los datos personales

La privacidad es una noción que desde siempre ha resultado imposible definir de manera exhaustiva, por cuanto es un concepto cuya densidad y contenido dependerá del tiempo y lugar en que se aplique.[179] **Lara** y otros se refieren a esta característica en los siguientes términos: "la privacidad se vincula a una manifestación jurídica del respeto y protección que se debe a cada persona, protegiendo la dignidad y libertad humana, por medio del reconocimiento a su titular de un poder de control sobre aquel ámbito del que no participan otras personas"[180]. En este mismo sentido **Herrán** sostiene que a través de la protección de la privacidad, "se aspira a garantizar el control de la información que nos concierne y que otros conocen de nosotros",[181]

[179] HERRÁN, ANA ISABEL (2003) *El derecho a la protección de los datos personales en la sociedad de la información*. En Cuadernos Deusto de Derechos Humanos, Universidad de Deusto: Bilbao, p. 9.

[180] LARA, J. CARLOS, et. al. La privacidad en el sistema legal chileno. En Policy Papers N° 08. Derechos Digitales. En línea en https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf, p. 12

[181] HERRÁN (2003) op. Cit. P.11

en cuantos se considera que "su revelación ocasionaría una perturbación en su dignidad como ser humano, y mermaría su desarrollo individual".[182]

Por tratarse de un poder de control, su contenido podrá enmarcarse en la protección de la vida privada, el secreto de las comunicaciones, la inviolabilidad de domicilio, la libertad de conciencia, la protección de datos personales, por mencionar algunos derechos que se han reconocido como directamente relacionados con la posibilidad de la persona de excluir de injerencias de terceros a estas esferas de su vida.

Es importante delimitar el contenido de cada uno de estos derechos, porque ello permitirá determinar el contenido esencial de cada uno de ellos y, con ello, poder delinear las injerencias que podrán ser toleradas por el legislador debido a la protección de otros intereses jurídicos confluyentes.

a. Protección de la privacidad a nivel internacional.

La **Declaración Universal de Derechos Humanos de la ONU** prescribe en su artículo 12 que "[n]adie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Exactamente lo mismo dispone el **artículo 17 del Pacto Internacional de Derechos Civiles y Políticos** (1966) y **la Convención sobre los Derechos del Niño en su artículo 16 (**1989). Respecto del primero, en 1988, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, redactó una Observación General, N°16, que, en definitiva, reconoció que la protección de la intimidad incluye la protección de datos personales.[183] En efecto, dicha observación señaló que "para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado."[184]

---

[182] Ibid.

[183] OFICINA DEL ALTO COMISIONADO DE LA ONU PARA LOS DERECHOS HUMANOS (1988) *Derecho a la intimidad (Art 17) HRC Observación general N°16.*

[184] Ibid. p. 2.

La **Convención Americana sobre Derechos del Hombre**, conocida como Pacto de San José de Costa Rica (1969), en su artículo 11° dispone algo bastante similar a los instrumentos anteriores:

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

La Corte Interamericana de Derechos Humanos sostiene que la "vida privada extiende sus alcances más allá del domicilio y la correspondencia, incorporando otros aspectos como la intervención, monitoreo, grabación y divulgación de conversaciones por vía telefónica".[185] Incluso, en el caso "Escher y otros contra Brasil", esta Corte reconoció que el artículo 11 de la Convención se aplica a las conversaciones telefónicas con independencia de su contenido, poniendo de ejemplo el origen y destino de la llamada, la identidad de los participantes, la frecuencia, hora y duración de las llamadas.[186]

En la Unión Europea el Tribunal Europeo de Derechos Humanos "reconoce que bajo el concepto de vida privada pueda quedar amparada 'toda información relativa a una persona física identificada o identificable' […] lo que a su vez es consistente con la amplia definición de dato personal".[187]

---

[185] MAQUEO, MARÍA SOLANGE; MORENO, JIMENA; RECIO, MIGUEL (2017) *Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario.* Revista de Derecho vol. XXX N° 1. P.83.

[186] RODRIGUEZ, KATITZA & ALIMONTI, VERIDIANA (2021) *A pesar del progreso, los metadatos aún tienen una protección de "segunda clase" en Latam.* EFF. Disponible en https://www.eff.org/es/deeplinks/2021/02/despite-progress-metadata-still-under-second-class-protection-latam-legal [Visto en línea 10/01/2022].

[187] Ibid. p. 88.

Por su parte, el Tribunal de Justicia de la Unión Europea ha reconocido una estrecha vinculación entre el derecho a la vida privada y el derecho a la protección de datos personales, pero acentuando el carácter autónomo de éste.[188]

b. Derecho a la vida privada en la Constitución de Chile.

Se encuentra consagrado en el N°4 del art. 19 de la CPR, al garantizar "el respeto y protección a la vida privada", entendida como el derecho a "excluir a terceros de nuestra esfera más íntima, sin imponer obligaciones jurídicas sobre ellos, salvo de no traspasar nuestra privacidad".[189]

La vida privada "se constituye por 'aquellos fenómenos, comportamientos, **datos,** y situaciones de una persona que normalmente están sustraídos del conocimiento de extraños y cuyo conocimiento de estos puede turbarla'."[190]

En cuanto a lo que concierne a si los datos de tráfico están o no protegidos por este derecho, se ha sostenido que "La privacidad no se encuentra limitada al contenido de nuestras comunicaciones. Los metadatos pueden entregar información incluso más completa que una conversación telefónica aislada".[191] Esto sería así porque los datos tráfico, a diferencia del contenido de las comunicaciones, son datos exactos, datos matemáticos, nítidos y fáciles de analizar.[192]

c. Derecho a la protección de datos personales.

El 16 de junio del año 2018, a través de la Ley 21.096, se incorporó al numeral 4° del artículo 19 de la C.P.R. la protección de los datos personales, consagrándose como derecho fundamental en nuestro ordenamiento jurídico:

Artículo 19. La Constitución asegura a todas las personas:

---

[188] Ibid. p. 89.

[189] MOLINA, OSCAR (2018) *La protección de datos personales es un derecho constitucional.* [En línea] < https://www.az.cl/la-proteccion-de-los-datos-personales-es-un-derecho-constitucional/> [Visto en línea 07/01/2022].

[190] LARA, CARLOS et. al. (2014) op. Cit. p.194.

[191] Ibid. 205.

[192] Ibid.

"4°. El respeto y la protección a la vida privada y a la honra de la persona y su familia, y asimismo, **la protección de sus datos personales.** El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley."

Se trata de un derecho fundamental de tercera generación, también llamados "derechos de la solidaridad que superan el ámbito individual y se refieren a cuestiones de interés general".[193]

La protección de los datos personales, también llamada "**autodeterminación informativa**" propende a la protección "de la persona respecto del tratamiento que terceros hacen de sus datos, para efectos de evitar que haya discriminaciones arbitrarias".[194] Doctrinariamente se distingue del derecho a la privacidad "en cuanto la protección de datos impone deberes jurídicos a terceros para hacer efectiva la reserva de información y control de datos".[195]

El término autodeterminación informativa fue acuñado por primera vez en 1983 por el Tribunal Constitucional Alemán, el cual sostuvo que el "derecho de la protección de datos ha de enmarcarse en el derecho general de protección de la persona, por considerar que garantiza la facultad del individuo a determinar por sí mismo la divulgación y utilización de datos referentes a su persona".[196]

Por otra parte, de la literalidad del precepto en cuestión, es posible apreciar que existe una reserva legal especial, por cuanto expresa que "el tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".[197] Entendemos que la regulación marco del tratamiento de datos se encuentra en la ley N°19.628 sobre Protección de la Vida Privada, pero además pueden haber otras leyes que regulen el tratamiento de datos en ámbitos específicos.

---

[193] HERRÁN (2003) op. cit. p. 13.

[194] DONOSO, LORENA (2020*) Primer Congreso Estudiantil de Derecho y Tecnología: Desafíos Tecnológicos en la nueva Constitución*. Facultad de Derecho Universidad de Chile. Disponible en https://www.youtube.com/watch?v=jNWzl55e0lI&t=6007s&ab_channel=uchilederecho [Visto en línea 20/11/2020].

[195] MOLINA (2018) Op. Cit.

[196] HERRÁN (2003) p. 14.

[197] ÁLVAREZ VALENZUELA, DANIEL (2020) *La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa.* Santiago: Revista Chilena de Derecho y Tecnología. Vol. 9, N°1, págs. 1-4. P. 2.

Con anterioridad a esta reforma, la protección de los datos personales se fundaba en el concepto genérico de protección a la vida privada, del mismo N°4. Incluso el Tribunal Constitucional había declarado que "la protección de la vida privada de las personas guarda estrecha relación con la protección de los datos personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa".[198]

La moción parlamentaria que inicia el proyecto que devino en la ley N°21.096, fundamenta la necesidad de una protección de los datos personales en el hecho de que la mayoría de los países que conforman la OCDE la consagran dentro de sus ordenamientos jurídicos. Así, hace referencia a la Unión Europea, España y Portugal y la jurisprudencia dictada en esos ámbitos. En la discusión se citó además la Constitución de Colombia[199], de Ecuador[200], de México[201]y, Brasil y Paraguay, países que a la época ya habían consagrado la acción Habeas Data a nivel constitucional.

Otro aspecto relevante es que en la historia de la ley se deja claro que la noción de autodeterminación informativa dice relación con "el derecho de las personas a controlar sus datos personales, incluso si éstos no se refieren a su intimidad."[202] Siendo así, el derecho a la protección de datos personales es incluso más amplio que el derecho a la privacidad, pues "el bien jurídico tutelado en la protección de datos no se identifica exclusivamente con la esfera privada de las personas" sino que "se extiende a garantizar otros valores y libertades de las personas".[203] La protección de datos personales "no se limita a datos íntimos, sino a cualquier información personal, sea o no íntima",[204] incluidos los de carácter público que puedan afectar a derechos y libertades de la persona.

---

[198] SENTENCIA DEL TRIBUNAL CONSTITUCIONAL (2011) Roles acumulados N°1732-10 y 1800-10 De 21 de junio de 2011, *sobre publicación de las remuneraciones de altos ejecutivos de Televisión Nacional de Chile.*

[199] Inciso 2° de su artículo 15.

[200] Habeas Data consagrado a nivel Constitucional en su artículo 92.

[201] Artículo 16.

[202] Moción Parlamentaria (2014) Boletín N°9.384-07: *Proyecto de reforma constitucional, iniciado en moción de los Honorables Senadores señores Harboe, Araya, Lagos, Larraín y Tuma, que consagra el derecho a la protección de los datos personales.* Chile.

[203] HERRÁN (2003) op. cit. p. 18

[204] Ibid. p. 21

En palabras del TC alemán, "lo decisivo en la protección de datos no es la naturaleza íntima o no del dato cuyo registro se pretende, lo verdaderamente relevante será la utilización, la finalidad del tratamiento o la posible interconexión de los datos personales tratados".[205] No se limita a datos íntimos, sino a cualquier información personal.[206]

Daniel **Álvarez** sostiene que [e]l derecho a la autodeterminación informativa es resultado de un doble proceso de transformación social y jurídica. Por una parte, la creciente utilización de tecnologías informáticas y digitales por parte de órganos del Estado, del sector privado y de la propia ciudadanía para la captura, procesamiento y transmisión de información personal, levantó varias alarmas respecto del impacto que este tipo de herramientas podía tener en la protección de los derechos fundamentales de las personas.[207]

En derecho comparado, el TC español ha declarado que el derecho a la privacidad se diferencia de la protección de datos personales en que el primero garantiza al individuo un ámbito de reserva, mientras la segunda permite a la persona ejercer un poder de control sobre la información personal, sobre su utilización y destino, para evitar utilizaciones ilícitas.[208] En resumen, el primero es de carácter pasivo y el segundo activo.

En este mismo sentido, Marianne **Díaz** sostiene que "el dato, como unidad mínima de información, puede no poseer o aportar una gran cantidad de significado por sí mismo, pero cobra un enorme sentido al ser correlacionado con otros puntos de información que, sumados, constituyen un perfil del usuario, de sus redes interpersonales y de su comportamiento en la sociedad y en el mercado".[209] Asimismo señala que las Naciones Unidas no consideran como necesaria o proporcional la retención de datos obligatoria por parte de operadores de telecomunicaciones, y que interfiere con el derecho a la privacidad.[210]

---

[205] Ibid. p. 14.

[206] Ibid. p. 21.

[207] ÁLVAREZ (2020) op. cit. p. 2.

[208] Ibid. p. 20.

[209] DÍAZ, MARIANNE (2017) *Retención de datos y registro de teléfonos móviles*. [en línea] Derechos Digitales. Chile. 9p. <https://www.derechosdigitales.org/wp-content/uploads/informe-marianne-retencion-de-datos.pdf> [Visto en línea 03/12/2029].

[210] Ibid.

4. Derecho a la inviolabilidad de las comunicaciones.

Artículo 19. "La Constitución asegura a todas las personas:

5°. La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos interceptarse, abrirse o registrarse en los casos y formas determinados por la ley."

Este derecho protege las comunicaciones privadas "entre personas, de las que no se pretende que su contenido se haga público, comprendiendo la protección de la correspondencia o de mensajes epistolares, telegráficos, telefónicos, radiales por télex o por otros medios, que la técnica haga posible ahora y en el futuro, que las personas llevan consigo, mantienen en su vivienda o en su trabajo y que sean dueñas o tenedoras legítimas".[211]

En palabras de Alejandro **Silva Bascuñán** al referirse a comunicación privada se entiende que "protege aquella forma de comunicación que dirige el emisor al receptor con el propósito de que únicamente él la reciba y ambos sepan su contenido; por lo tanto, se prohíba a otras personas imponerse de éste, a menos que el receptor consienta en que ello ocurra."[212]

Ahora bien, en este punto, cabe preguntarse si los datos de tráfico pueden considerarse comunicaciones y, por consiguiente, si son protegidos por el precepto legal en cuestión.

En este sentido, el **Tribunal Constitucional** se ha pronunciado señalando que los datos de tráfico se encuentran protegidos por el derecho a la inviolabilidad de las comunicaciones. En efecto, el Tribunal sostuvo que: "Lo que esta garantía protege es la comunicación, cualquiera sea su contenido y pertenezca o no éste al ámbito de la privacidad o intimidad. El secreto se predica respecto de la comunicación. Por lo mismo, abarca el mensaje y los datos de tráfico (ruta, hora, fecha, sujetos, etc.)". [213]

Los datos de tráfico, según diversos autores, también se encuentran protegidos mediante el derecho a la inviolabilidad de las comunicaciones.

---

[211] VIVANCO, ÁNGELA (2006) *Curso de Derecho Constitucional: aspectos dogmáticos de la Carta Fundamental. Tomo II, 2° edición.* Santiago de Chile: Ediciones Universidad Católica de Chile. p. 396

[212] SILVA BASCUÑÁN, ALEJANDRO (2006) *Tratado de Derecho Constitucional, tomo XI. 2° Edición*. Santiago de Chile: Editorial Jurídica de Chile. p.205

[213] TRIBUNAL CONSTITUCIONAL (2011) Sentencia rol 2153-2011, 11 de septiembre de 2012, sobre Acceso a la Información Pública y correos electrónicos considerando trigésimo primero.

Para Alejandro **Ivelic** los datos asociados cabrían bajo el marco de la inviolabilidad de las comunicaciones debido a que se trata de un derecho amplio, en el entendido de que la disposición constitucional es numerus apertus, que incluye cualquier medio o soporte tecnológico.[214]

De esta forma, el derecho al secreto de las comunicaciones protege además los datos asociados a la transmisión de comunicaciones que tienen por función comprobarla y registrarla, por ejemplo, registro de llamadas, registro de duración, fecha, ubicación, etc.[215]

En el derecho comparado alemán, los datos IMSI/IMEI "forman parte de la definición de comunicaciones, según la Ley de Telecomunicaciones, y, por lo tanto, su captura debería ser comprendida por la garantía que protege el secreto de las comunicaciones".[216]

2. El fallido Decreto Supremo N°866 de 2017.

El Decreto Supremo 866, que estableció el Reglamento sobre Interceptación de Comunicaciones Telefónicas y de otras formas de Telecomunicación, y Conservación de Datos Comunicacionales, data de 13 de junio de 2017, coloquialmente conocido como "**Decreto Espía"** tenía por propósito sustituir el Reglamento de 2005 sobre tales materias -Decreto Supremo N°142 de 2005-. Nótese que es anterior a la inclusión de la garantía constitucional de protección de datos personales, que data de 2018.

En las consideraciones previas del mismo, se incluyó como fundamento, que la Constitución Política "garantiza a todas las personas la inviolabilidad de todo tipo de comunicación privada, permitiendo su interceptación solo en los casos y formas determinados por la ley".[217]

Asimismo, se fundó en la necesidad de mejorar el procedimiento de interceptación de las comunicaciones que regula el mencionado Decreto Supremo N°142, estableciendo un

---

[214] IVELIC MANCILLA, ALEJANDRO. (2014) Las interceptaciones de comunicaciones telefónicas en los delitos de tráfico ilícito de estupefacientes. Revista Jurídica del Ministerio Público. N° 60, septiembre 2014. P. 109.

[215] Ibid. p. 110.

[216] ROLÓN, DARIO (2017) I*ntercepción de metadatos de comunicaciones por teléfonos móviles. El IMSI-Catcher y su regulación en el ordenamiento procesal penal alemán.* Revista de Estudios de Justicia, N°27, Santiago. p. 77.

[217] PRESIDENTE DE LA REPÚBLICA (2017) *Proyecto de Decreto Supremo 866 de 2017*. [en línea] Disponible en: < https://www.derechosdigitales.org/wp-content/uploads/decreto-866-2017.pdf> [Visto en línea 08/02/2021] p. 1.

"procedimiento de carácter general, aplicable a todos los proveedores de servicios de telecomunicaciones", de forma tal que se detallara y especificaran los deberes que les corresponderían a tales operadores respecto de la interceptación de las comunicaciones y de la conservación de los "datos comunicacionales" que fueran importantes para el "cumplimiento de los cometidos de los órganos del Estado", mencionando especialmente al Ministerio Público.[218]

Sin embargo, el Decreto Supremo N°866 de 13 de junio de 2017 no podía prosperar porque era inconstitucional, al incluir materias que sólo podían regularse por ley y no a través de normas de rango inferior[219], por lo que fue representado por la Contraloría General de la República.[220]

Entre lo cuestionado, la propuesta de Reglamento establecía una regulación mucha más detallada que el de 2005, tanto de la interceptación de las comunicaciones como de la preservación de datos de tráfico. En este último aspecto, el Título III, denominado "Conservación de datos", contenía los artículos 8°, 9°, 10°, 11° y 12°, con los contenidos que esbozamos a continuación:

El artículo 8° establecía que las empresas de telecomunicaciones tendrían la obligación de conservar los datos de tráfico por un periodo mínimo de 2 años.

El **artículo 10°** elaboraba una extensa lista de la información mínima que debía conservarse, incluyendo:

a) Los antecedentes del suscriptor y/o usuario que permitan conocer los datos administrativos y financieros de los mismos, sea la forma y medio de pago que utiliza el periodo de habilitación y tipo de servicio, entre otros.

b) Los antecedentes necesarios para identificar el origen de la comunicación, tales como número de teléfono, nombre y datos del suscriptor, dirección IP, entre otros.

c) Los antecedentes necesarios para identificar el destino de la comunicación.

---

[218] Ibid. p. 1 -2.

[219] Instituto Chileno de Derecho y Tecnologías. (2017) *Presentación a la Contraloría General de la República.* Disponible en línea < http://www.icdt.cl/wp-content/uploads/2017/08/peticion-CGR-30agosto.pdf > [Visto en línea 10/10/2020].

[220] ICDT (2017) "En efecto debe objetarse que diversas disposiciones del señalado reglamento regulan materias propias de ley, como lo son las relativas a la conservación de datos comunicacionales por parte de los prestadores de servicios de telecomunicaciones…" <http://www.icdt.cl/wp-content/uploads/2017/11/CGR-representa-decreto-espia.pdf> [Visto en línea 10/10/2020].

d) Los antecedentes para determinar la fecha, hora y duración de la comunicación.

e) Los antecedentes para determinar la clase o tipo de comunicación.

f) Los antecedentes para terminar los equipos terminales intervinientes en la comunicación, y su ubicación geográfica con las indicaciones y requisitos que exija la norma técnica respectiva.

g) Cualquier otra información requerida por la Norma Técnica respectiva y que sirva para complementar los antecedentes requeridos en las letras anteriores.

Previo a su publicación, el Decreto debía ser sometido al procedimiento de toma de razón de la Contraloría General de la República -en virtud de los deberes que le impone el artículo 10 de la ley N°10.336 de Organización y Atribuciones de la Contraloría General de la República- que consiste en un control preventivo de constitucionalidad y legalidad de los decretos supremos dentro del plazo de quince días contados desde la fecha de su recepción. En el curso de este trámite, el Instituto Chileno de Derecho y Tecnologías (en adelante ICDT) -representados por el abogado Raúl Arrieta Cortés-, solicitó a la Contraloría que se tuviera presente las distintas diferencias que existían entre el artículo 222 del C.P.P. y el Decreto en cuestión. Así, por ejemplo, enfatizó en que el Decreto permitía que los datos comunicacionales fueran puestos a disposición de **cualquiera autoridad a que una ley proporcionara facultades para solicitarlos** (Artículo 8°); en cambio, el inciso quinto del artículo 222 del C.P.P. lo permite solo respecto del Ministerio Público. Adicionalmente, el decreto no establecía la necesidad de una autorización judicial.

En tercer lugar, señalaron que los **plazos mínimos de conservación**, que se incluían eran de un año y dos respectivamente. [221] Finalmente, observan que mientras el C.P.P. menciona solamente los números IP de las conexiones de sus abonados, el **contenido sometido a conservación**, señalado en el Decreto, incluía una lista bastante más amplia en su artículo 10.[222] De estas observaciones el ICDT concluyó que existía el riesgo de que lo que entonces venía siendo una excepción a la inviolabilidad del hogar y de toda forma de comunicación privada, degeneraría en un "sistema general de vigilancia de la población del país", considerándose desproporcionado

[221] Ibid.

[222] Ibid.

e “incompatible con la existencia y desarrollo de un sistema democrático y respetuoso de los derechos fundamentales”,[223] toda vez que vulnera no solo la inviolabilidad del hogar y de toda comunicación privada, sino que además el libre desarrollo de la personalidad, como expresión de la libertad que garantiza el artículo primero de la C.P.R., en el entendido de que “no se comporta de la misma forma quien es libre respecto de los que están sometidos a vigilancia”.[224]

Luego, se señalan como infringidos los artículos 6 y 7 de la C.P.R, donde se consagra el principio de legalidad y la supremacía constitucional, pues las normas propuestas infringían el tenor literal del 222 del C.P.P., referirse a materias que son de “reserva legal absoluta”, esto es, que solo el legislador puede regularlas, no así el ejecutivo, sin que se permitan disposiciones legales genéricas e indeterminadas.[225]

Otro argumento que menciona el Instituto es que se “rompe con la presunción de inocencia que garantiza a todas las personas el artículo 19N°3 de la Constitución y los artículos 4 y5 del C.P.P.”, toda vez que establece la obligación de tener a disposición de cualquiera autoridad, información detallada de los datos personales de las personas, por un periodo mínimo de dos años, que resultaría “desproporcionado”. En este sentido argumenta que se invertiría la situación de que las personas son inocentes hasta que se demuestre lo contrario.[226]

Concluye el ICDT solicitando a la Contraloría que represente, es decir, que no tome razón de dicho Reglamento, enfatizando en que el Decreto es inconstitucional por las razones precedentes, y que se trata de asuntos que son materia exclusivamente de ley que, además se encuentran en contradicción con la norma de rango legal que es el artículo 222 del C.P.P.

Finalmente, con fecha 24 de noviembre de 2017, la Contraloría General de la República, a través de un escueto Dictamen, representó el Decreto en cuestión, señalando que éste no se ajustaba a derecho, por cuanto “diversas disposiciones” regulaban “materias propias de ley,” refiriéndose a “las relativas a la conservación de datos comunicacionales por parte de los prestadores de servicios de telecomunicaciones, y a las atribuciones de los jueces de garantía y Ministerio

[223] Ibid. P.4.

[224] Ibid.

[225] Ibid.

[226] Ibid.

Publico, excediendo normas de Código Procesal Penal que se invocan como fundamento o resultan aplicables"[227]

Además, indicó que los términos amplios con que se refería a las autoridades capaces de requerir la información no se justaban a los que las leyes se refieren, por ejemplo, al Ministerio Público en el art 222 C.P.P.[228]

3. Proyecto de ley: Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N°11.144-07.

El 15 de marzo de 2017, se ingresó, por vía de mensaje presidencial, el proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

Dicho mensaje (N°001-365), consta de una estructura que inicia con antecedentes generales, que hacen referencia del desarrollo de la **economía digital** y **contexto internacional.**

Respecto de la **económica digital**, el mensaje indica que el paso de una sociedad industrial a una digital ha significado una expansión de los espacios de libertad, autonomía y desarrollo de la persona, pero que, a la vez, ha venido de la mano con sistemas de control y vigilancia de mayor precisión, que amenazan o limitan tal libertad. Por consiguiente, la sociedad y el estado deben propender a establecer un equilibrio entre ambos aspectos, el primero, la libertad individual, y segundo, el interés público. A continuación, se refiere a la falta en Chile de una legislación que esté a la altura de las normas y estándares internacionales en materia de protección y tratamiento de datos personales.[229]

En seguida, el mensaje se refiere al ingreso de Chile, en el año 2010, a la Organización para la Cooperación y el Desarrollo Económico (OCDE), indicando que el proyecto viene a adoptar las

---

[227] CONTRALORÍA General de la República. 24 de noviembre de 2017. Dictamen 041188N17. Representa el decreto N° 866, de 2017, del Ministerio del Interior y Seguridad Pública <https://www.contraloria.cl/pdfbuscador/dictamenes/041188N17/html> [Visto en línea 18/11/2019] p.1.

[228] Ibid. p.2.

[229] [229] MENSAJE PRESIDENCIAL (2017) Boletín N°11.144-07: *Proyecto de ley, iniciado en mensaje de S. E. la Presidenta de la República, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales* [en línea] Ingresado el 11 de marzo de 2017. p. 1-2 <https://www.camara.cl/verDoc.aspx?prmID=11456&prmTIPO=INICIATIVA> [Visto en línea el 26/04/2020].

recomendaciones que dicho organismo ha efectuado sobre respeto a la privacidad y flujo transfronterizo de datos personales.[230]

El proyecto de ley se funda, también, en el derecho fundamental a la vida privada y su protección, haciendo referencia a las falencias de la Ley 19.628, que el avance de las tecnologías ha develado.[231] En adición a esto, se menciona cómo la Corte Suprema se ha referido a los derechos fundamentales que entran juego, a saber, "vida privada, intimidad, honra, libertad de opinión e información, acceso a la información y transparencia, entre otros".[232]

En cuanto al **objetivo general** del proyecto señala que es "actualizar y modernizar el marco normativo e institucional con el propósito de establecer que el tratamiento de los datos personales de las personas naturales se realice con el consentimiento del titular de datos o en los casos que autorice la ley, reforzando la idea de que los datos personales deben estar bajo la esfera de control de su titular, favoreciendo su protección frente a toda intromisión de terceros y estableciendo las condiciones regulatorias bajo las cuales los terceros pueden efectuar legítimamente el tratamiento de tales datos, asegurando estándares de calidad, información, transparencia y seguridad".[233] Así, se pretende que haya mayor claridad y equilibrio entre la protección de la vida privada e intimidad de las personas, y, por el otro lado, la libre circulación de información.[234]

En cuanto al contenido del proyecto, se pueden sintetizar de la siguiente manera:

a. Determinación precisa del ámbito regulatorio.

El artículo 1° del proyecto de ley se refiere al objeto y ámbito de aplicación de la ley. Mientras el primero es "el tratamiento de datos personales que realicen personas naturales y jurídicas, públicas o privadas, con el propósito de asegurar el respeto y protección de los datos derechos y libertades de quienes son titulares de estos datos, en particular, el derecho a la vida privada",

[230] Ibid. p.3.

[231] Ibid.

[232] Ibid.p4.

[233] Ibid. p.4.

[234] Ibid.

el ámbito de aplicación es todo tratamiento de datos que no esté regulado por una ley especial. Se pretende, por lo tanto, que esta ley sea un marco regulatorio para todos aquellos aspectos que no tienen una regulación específica.

b. Principios rectores y actualización de definiciones legales.

Los principios rectores tienen por función orientar el sentido de las disposiciones legales de cara a la interpretación doctrinaria y jurisprudencial de las mismas. En el caso del proyecto de ley en análisis se mencionan los siguientes:

1. Principio de licitud del tratamiento: Supone que los datos solo pueden tratarse con el consentimiento de su titular o por disposición de la ley.
2. Principio de finalidad: los datos deben ser recolectados con fines específicos, explícitos y lícitos y su tratamiento limitarse a estos fines; quedando, además, prohibido el tratamiento de datos para un fin distinto al que el titular entregó su consentimiento.
3. Principio de proporcionalidad: Los datos a tratar deben limitarse a aquellos que resulten necesarios a los fines. Además, los datos deben conservarse solo por el periodo necesario para dichos fines, salvo autorización legal o consentimiento del titular.
4. Principio de calidad: Los datos deben ser exactos, completos y actuales en relación con los fines del tratamiento.
5. Principio de seguridad: Se deben garantizar niveles adecuados de seguridad para el tratamiento de los datos, de manera que se minimicen los riesgos de tratamiento no autorizado, pérdidas, filtraciones, destrucciones o daño accidental.
6. Principio de responsabilidad: Serán legalmente responsables del cumplimiento de los principios, obligaciones y deberes de conformidad con el proyecto de ley.
7. Principio de información:[235]Debe permitirse permanentemente el acceso a las prácticas y políticas sobre el tratamiento de datos personales y estar a disposición de cualquier interesado de manera detallada y específica.

[235] Ibid. p.5.

Asimismo, se incorporan principios específicos que rigen el tratamiento de datos personales por organismos públicos:

a) Principio de coordinación.

b) Principio de eficiencia.

c) Principio de transparencia.

d) Principio de publicidad.

c. Reforzamiento y ampliación de los derechos de los titulares de datos:

Se reconocen los derechos de acceso, rectificación, cancelación y oposición (Derechos "ARCO"), estableciendo un procedimiento de resguardo. Asimismo, regula la portabilidad de los datos personales. Finalmente se refuerza el ejercicio del derecho al olvido respecto de información que se refiera a materias penales y otras.[236]

d. Consentimiento del titular como la principal fuente de legitimidad del tratamiento de datos

Dicho consentimiento debe tener las cualidades de ser "libre, informado, inequívoco, otorgado en forma previa al tratamiento y específico en cuanto a su finalidad".[237] No obstante, establece excepciones a esta regla general, por ejemplo, **cuando sea necesario para el cumplimiento de una obligación legal o contrato en que forme parte su titular.**

e. Régimen de responsabilidades de los responsables de datos

Se establecen deberes de información, de reserva y confidencialidad, de información y transparencia, y deber de adoptar medidas de seguridad y reportar las vulneraciones. Distinguiendo entre personas naturales y jurídicas, y su tamaño. Finalmente se regula la cesión y transferencia de las bases de datos y del tratamiento de Big Data.

[236] Ibid. p.6.

[237] Ibid. p.7.

f. Nuevos estándares para el tratamiento de datos sensibles y categorías especiales de datos personales

Se exige consentimiento expreso para el tratamiento de datos sensibles, salvo que sean públicos o se requieran por emergencia de salud. Además, se regulan diferenciadamente los datos biométricos, estadísticos, **de geolocalización**, etc.[238]

g. Tratamiento de datos personales de niños, niñas y adolescentes

Permitido solo en favor del interés general del niño y el respeto de su autonomía progresiva, diferenciando entre niños y adolescentes, debiéndose velar por su protección.

h. Regulación del flujo transfronterizo de datos personales

En resumen, se eleva el estándar nacional a las recomendaciones de la OCDE y UE, distinguiendo entre países con niveles adecuados de protección frente a los que no, siendo más estrictos con éstos.

i. Modernización de estándares para el tratamiento de datos personales por organismos públicos.

Se establece que en los casos en que los organismos públicos actúen según su función legal, dentro del ámbito de sus competencias y de conformidad con las normas legales correspondientes, no necesitarán consentimiento del titular para el tratamiento de datos, pudiendo, los organismos públicos, ceder tales datos a otros órganos públicos. Como contrapartida se establece para titular un procedimiento de reclamación administrativa y de tutela judicial efectiva para la protección de sus derechos.[239]

Se regula un régimen excepcional para datos protegidos por el secreto profesional, cuando se trata de datos relacionados a la investigación de infracciones penales, civiles y administrativas;

[238] Ibid. p.8.

[239] Ibid. p.9.

seguridad de la Nación, orden o seguridad públicos; y en caso de declaración de estado de catástrofe o de emergencia.[240]

j. Artículos que interesan a esta esta investigación

En cuanto a su articulado, nos interesa mencionar algunas generalidades y disposiciones relacionadas con el tratamiento de datos de tráfico.

El proyecto hace modificaciones respecto de las definiciones que establece el artículo segundo de la ley N°19.628:

"**c) Comunicación o transmisión de datos personales:** "Comunicación o transmisión de datos personales: dar a conocer por el responsable de datos, de cualquier forma, datos personales a personas distintas del titular a quien conciernen los datos, sin llegar a cederlos o transferirlos."

f) Dato personal: "cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular **mediante uno o más identificadores**, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, excluyendo aquellos casos en que el esfuerzo de identificación sea desproporcionado."

g) Datos personales sensibles: <u>sólo</u> tendrán esta condición aquellos datos personales que revelen el origen étnico o racial, la afiliación política, sindical o gremial, hábitos personales, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural.

[240] Ibid. p.10.

El artículo 12, dispone que se requiere del consentimiento del titular para realizar el tratamiento de sus datos. Señala además que el consentimiento debe ser libre, informado especifico en cuanto a su finalidad e inequívoco.

El artículo 13 letra c) establece que es lícito el tratamiento cuando "sea necesario para la ejecución o el cumplimiento de una obligación legal o **lo disponga la ley**". En este sentido, ley que dispone el tratamiento de datos en relación con los datos de tráfico es el ya mencionado artículo 222.

A efectos de este trabajo, es relevante el Título IV, concerniente al tratamiento de datos personales por los órganos públicos, compuesto por los artículos 20 a 26.

El artículo 20 consagra la regla general del tratamiento de datos por órganos públicos, que se resume en que no requiere del consentimiento del titular para tratar sus datos, siempre que los órganos obren para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias.

A continuación, el **artículo 21** establece los principios que rigen el tratamiento de datos por órganos públicos que, además de los que consagra el artículo 3°, agrega los **principios de coordinación, eficiencia, transparencia y publicidad**. El primero se refiere a la interoperabilidad que debe haber entre distintos organismos, de forma que se eviten contradicciones y reiteraciones innecesarias de requerimientos de información. El principio de eficiencia consiste en la evitación de duplicación de procedimientos y tramites entre la diversidad de organismo, incluyendo los particulares. Conforme a los principios de transparencia y publicidad, los organismos públicos deben permitir el acceso a la información que tengan en su poder, propendiendo resguardar los derechos de las personas afectadas, de conformidad con el artículo 20 de la Ley de Transparencia contenido en el artículo primero de la ley N°20. 285

El artículo 24 letra b) establece que **no se aplican los artículos de la ley a los órganos públicos "[c]uando realicen tratamiento de datos personales para la investigación, persecución, enjuiciamiento o sanción de infracciones penales, civiles y administrativas**.", pero deberá

cumplirse siempre con los "principios licitud del tratamiento, calidad, seguridad y responsabilidad".[241]

Con posterioridad, durante la tramitación del proyecto la disposición anteriormente transcrita fue sujeta a modificaciones en su redacción. Así consta en el segundo informe de comisión, de 16 de marzo de 2020, que propone el siguiente texto:

"Artículo 24. Regímenes especiales. El tratamiento, comunicación o cesión de datos personales, realizado por órganos públicos competentes en las materias que a continuación se indican, estarán sujetos exclusivamente al régimen de regulación especial establecido en este artículo:

a) Aquellos que se realicen con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas las actividades de protección y prevención frente a las amenazas y riesgos contra la seguridad pública."

Al mismo artículo, le son agregados incisos nuevos al final, que obligan a los organismos públicos a tratar los datos siempre para el cumplimiento de sus funciones legales, dentro del ámbito de sus competencias y respetando las garantías fundamentales del artículo 19N°4 de la C.P.R. y los principios establecidos en el artículo 3°.

Esta disposición hay que relacionarlas con el inciso cuarto artículo 14 bis propuesto, que señala lo siguiente:

"Quedan sujetas a la obligación de secreto o confidencialidad las personas e instituciones y sus dependientes, que en cumplimiento de una obligación legal han remitido información a un organismo público sujeto al régimen de excepciones establecido en el artículo 24, en cuanto al requerimiento y al hecho de haber remitido dicha información."

De esta forma se reforzaría el deber de confidencialidad establecido en el inciso quinto del artículo 222 del CPP.

Otra norma interesante se encuentra en el artículo 16 sexies que regula el tratamiento de datos de geolocalización:

[241] Artículo 24, inciso final.

"Artículo 16 sexies. - Datos de geolocalización. El tratamiento de los datos personales de geolocalización del titular se podrá realizar bajo las mismas fuentes de licitud establecidas en los artículos 12 y 13.

El titular de datos deberá ser informado de manera clara, suficiente y oportuna, del tipo de datos de geolocalización que serán tratados, de la finalidad y duración del tratamiento y si los datos se comunicarán o cederán a un tercero para la prestación de un servicio con valor añadido."

De esta manera se sujeta el tratamiento al requisito de consentimiento del titular de los datos, salvo los casos enumerados en el artículo 13, donde no se requiere.

Actualmente este proyecto de ley se encuentra en segundo trámite constitucional.

4. Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest.

El 25 de octubre de 2018 se ingresó al Senado, a través de un mensaje presidencial, este proyecto de ley, que tiene por finalidad actualizar la normativa interna al Convenio de Budapest ya vigente en nuestro país y terminar con los vacíos legales que padece la ley 19.223, para establecer una actualización del catálogo de delitos informáticos.

Junto con lo anterior, el proyecto pretende modificar el CPP en orden dotarlo de mayor eficacia. Así, por ejemplo, el mensaje presidencial señala que las herramientas de persecución penal respecto a esta materia "han devenido insuficientes para una adecuada investigación".[242] También hace referencia a la necesidad de complementar el Convenio de Budapest con una "normativa procesal que entregue recursos que permitan investigaciones eficaces" para la ciberdelincuencia.[243]

En lo que interesa a esta investigación, cabe señalar que se modifica el artículo 222 del CPP, estableciendo, entre otras novedades, la obligación de retener datos relativos a tráfico, junto con

[242] BOLETÍN N°12.192-25 (2018) *Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest*. P. 4.

[243] Ibid. p. 5.

entregar la definición de este tipo de dato. De hecho, se reemplaza el actual epígrafe del artículo por el de "intervención de las comunicaciones y conservación de los datos de tráfico".

La nueva redacción propuesta del inciso quinto del artículo 222 agrega la obligación de mantener con carácter reservado, por un plazo no inferior a dos años, los correspondientes datos relativos a tráfico, como también los domicilios y residencia de sus clientes.

7.1. Definición de datos de tráfico

Respecto de la definición de datos de tráfico, el propuesto inciso sexto señala que para efectos de ese artículo se "entenderá por datos relativos a tráfico, todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, la localización del punto de acceso a la red, el destino, la ruta, la hora, la fecha, el tamaño y duración de la comunicación o el tipo de servicio subyacente".[244]

7.2. Informe sobre el proyecto de ley elaborado por la Corte Suprema.

Según un informe acerca del proyecto, realizado por la Corte Suprema, no queda claro "cuáles comunicaciones pasan a regirse por cada uno de los artículos, esto es, si se rigen por el 219 CPP todas aquellas que no han sido expresamente contempladas en el 222 CPP".[245] Todo ello por cuanto se propone para el artículo 222 que se agregue que se tenga un listado de datos relativos al tráfico, pero sólo respecto a direcciones IP. Nada dice respecto a llamadas telefónicas.

Como consecuencia la Corte Suprema recomienda que debiese regularse a través de distintos artículos o disposiciones las tres materias en cuestión, a saber, (1) información relativa a comunicaciones privadas en poder de empresas operadores de telecomunicación; (2) información relativa a comunicaciones públicas en poder de empresas de telecomunicación,

[244] Artículo 14 del proyecto de ley.

[245] CORTE SUPREMA. 12 de febrero de 2019. *Oficio N° 23 – 2019. Informe proyecto de Ley N° 2-2019*. [en línea] Antecedente: Boletín N° 12.192-25 <https://www.pjud.cl/documents/396729/0/INFORME+PROYECTO+DE+LEY+CONVENIO+BUDAPEST.pdf/f1b87b83-ee25-4ff7-b605-925f5319577e> [Visto en línea 01/12/2019].

prensa y radiodifusión; y (3) el ámbito de interceptación de mensajes y comunicaciones privadas sujetas a reserva.

Al pronunciarse respecto de metadatos, datos de tráfico o contexto, la Corte señala que "no obstante ser externos al contenido del mensaje pueden poner en riesgo, también, la privacidad de la persona".[246]

A raíz de esta confusión que vislumbró la Corte Suprema, el 22 de diciembre de 2020, la Presidencia de la República formuló indicaciones al proyecto a través del Oficio N°489-368, donde se propuso una nueva redacción para el artículo 219, relativo a copias de comunicaciones, transmisiones y datos informáticos; estableciendo en este artículo lo que antes se proponía en el artículo 222, acerca de la conservación de datos de tráfico, ahora por un plazo máximo de un año. Asimismo, la redacción del 219 establece la posibilidad del Ministerio Público de requerir, previa autorización judicial, que se entregue la información que se tenga relativa al tráfico y contenido de las comunicaciones de los abonados de las empresas de telecomunicaciones, entre otras regulaciones.

Actualmente el proyecto se encuentra en tercer trámite constitucional, donde se hace presente la urgencia Suma.[247]

[246] Ibid.

[247] 07/06/2021.

Capítulo IV: Derecho comparado sobre tratamiento de datos personales de localización y tráfico de comunicaciones electrónicas.

En este capítulo se analizarán algunas experiencias de derecho comparado, que permiten ilustrar la insuficiencia de la legislación nacional, a la vez que aportar al debate con algunas propuestas que se podrían elaborar a partir de las experiencias que se reseñan.

1. Marco jurídico de la Unión Europea.

a. Directiva 2002/58/CE del Parlamento Europeo y del Consejo.

La Directiva 2002/58/CE, del Parlamento y Consejo Europeo, "relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)" de 12 de julio de 2002, contiene normas relevantes al objeto de nuestra investigación. En su **artículo 1**, dispone que la **finalidad** de la directiva es armonizar las legislaciones de los Estados miembros en orden a garantizar un nivel de protección del derecho a la intimidad y la libre circulación de los datos y de los equipos y servicios de comunicaciones electrónica en la Comunidad Europea, sin embargo, el inciso tercero del mismo artículo, relativo a su ámbito de aplicación, excluye la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal. Siendo así, en principio, no debería regular el tratamiento de datos en el ámbito de la investigación de delitos. Sin embargo, la Directiva 2006/24/CE en su apartado 15 revierte esta situación, según veremos más adelante.

En lo que nos interesa, el artículo 2 de la Directiva 2002/58/CE, en su letra b) define los "datos de tráfico" como "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma."

A continuación, en la letra c) del mismo artículo, define lo que son los datos de localización como "cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible al público."

Adicionalmente, la Directiva, en su artículo 9, clasifica los datos de localización en aquellos de tráfico o "datos de cobertura", que son aquellos que utilizan los operadores de comunicaciones para "poder hacer efectiva la eventual comunicación"[248], por lo que son accesorios a la comunicación como tal, y quedan registrados en el C.D.R. y los "datos de localización distintos de los de tráfico", que a su vez se subdividen en aquellos "datos de cobertura sin comunicación" que registran la localización haya o no comunicación, a través de la conexión permanente con el sistema, registrado mediante el HLR o *Home Location Register* y los "datos de localización como servicios de valor añadido", que son los GPS u otros, utilizados para realización de servicios básicos, y que requieren el consentimiento del usuario.[249]

b. Directiva 2006/24/CE del Parlamento Europeo y del Consejo.

Posteriormente se dictó la Directiva 2006/24/CE[250], "sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE", que tuvo por finalidad establecer un marco jurídico mínimo para los Estados miembros, de forma que los datos se encontraran "disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro. [251]

En cuanto al **ámbito de aplicación de la Directiva**, el artículo 1.2 habla por sí solo: "se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas."

---

[248] CABELLO GIL, LAURA M. (2017) *Datos de geolocalización como medida de investigación. Avances en el sistema jurídico procesal penal*. Tesis Doctoral. España, Facultad de Derecho de Universidad Nacional de Educación a Distancia. p.87.

[249] Ibid. 88.

[250] PARLAMENTO EUROPEO Y CONSEJO (2006) *Directiva 2006/24/CE, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, DOUE*, núm. 105, de 13 de abril de 2006.

[251] Art. 1.1 Directiva 2006/24/CE.

El **artículo 2** se pronuncia respecto de la aplicabilidad de las definiciones de la directiva 2002/58/CE, a las cuales nos referimos anteriormente y agrega la definición de datos siguiente: a) «datos»: los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario. Esta definición se condice con el apartado 2 del artículo 1, que deja afuera el contenido de las comunicaciones.

En el **artículo cuarto,** en materia de principios que los Estados miembros deben adoptar internamente, se prevé que el acceso a los datos debe llevarse a cabo por autoridades competentes, en caso específicos y de conformidad con su legislación nacional. Adicionalmente que todo Estado debe definir un procedimiento que se conforme con los principios de **necesidad y proporcionalidad,** teniendo en cuenta incluso la interpretación del Tribunal Europeo de Derechos Humanos respecto de estos principios.[252]

El **artículo quinto** enumera una lista esquematizada y pormenorizada de los datos que deberán conservarse, dentro los que se encuentran, el número de teléfono de llamada; el nombre y la dirección del abonado o usuario registrado; números de destino; IMSI e IMEI de quien llama; identificador de celda; entre otros.[253]

Respecto de la conservación de datos, la Directiva 2006/24/CE establece que la obligación de conservar datos incluye aquellos que son producto de **llamadas infructuosas**, es decir, aquellas en que el equipo terminal que la recibe no contesta o que "ha habido una intervención del gestor de la red"[254]. No obstante, no se incluyen las **llamadas no conectadas**.[255]

En cuanto al **periodo de conservación**, el artículo 6° establece que los estados deben garantizar que su duración sea de un tiempo no inferior a seis meses y ni superior a dos años.

En seguida se establecen obligaciones mínimas de seguridad y protección, en cuanto a la custodia y la obligación de destruir los datos una vez terminado el periodo de conservación.[256] No obstante queda abierta a la posibilidad de que, para enfrentar circunstancias especiales, se

[252] Art. 4 Directiva 2006/24/CE.

[253] Artículo 5 Directiva 2006/24/CE.

[254] Art. 2 f).

[255] Art. 3.2 Directiva 2006/24/CE.

[256] Art. 7.

amplíe este periodo, teniendo la obligación de informar y justificar la ampliación ante la Comisión y los Estados miembros, según lo estipula el artículo 12. Varios son los Estados miembros que manifestaron reservas en cuanto al periodo que el artículo 6° establece; entre ellos los Países Bajos, Austria, Estonia, etc., ya fuera para aplazar su aplicación o bien ampliar dicho periodo.[257]

En el artículo 11 de la Directiva 2006/24/CE, que modifica el artículo 15 de la Directiva 2002/58/CE, consagra la aplicabilidad de este cuerpo normativo, sin perjuicio de establecer la conservación de datos obligatoria, a diferencia de la situación anterior en que la conservación de datos era una excepción, no obligatoria para los Estados miembros.

En todo caso, debemos considerar que la Directiva 2006/24/CE, fue declarada nula por la sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, el 8 de abril de 2014, teniendo por fundamento la escasa claridad de sus normas en relación a las garantías jurídicas relativas al derecho de protección de datos personales.[258] El Tribunal declaró que se vulnera el derecho al respeto de la vida privada y familiar, y el derecho a la protección de datos personales, garantizados en la Carta de los Derechos Fundamentales de la Unión Europea, dado que no establece bien los fines concretos del tratamiento de datos.[259]

Según **Cabello** Gil, la resolución no distingue respecto de personas amparadas por el secreto profesional, tampoco hace excepciones respecto de la persecución de delitos graves. Careciendo, además de criterio objetivo para delimitar el acceso a autoridades.[260]

[257] Declaraciones al final de la Directiva 2006/24/CE.

[258] Ibid.

[259] Ibid.

[260] Ibid. 108.

2. Marco jurídico español.

a. Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Esta ley incorporó al derecho español la normativa europea, especialmente la directiva 2006/24/CE del Parlamento Europeo y del Consejo. En sus normas trata de equilibrar las medidas tendientes a proteger la seguridad pública con el respeto de derechos fundamentales, especialmente la privacidad e intimidad. En este sentido vino a consolidarse el lineamiento jurisprudencial que establecía que el tratamiento de los datos vinculados jamás incluyera el contenido de las comunicaciones como tales; y, en segundo lugar, que para llevarlas a cabo se requiriera de autorización judicial previa.

Con anterioridad a esta ley, las investigaciones tenían cortapisas frente al requerimiento de metadatos de las telecomunicaciones, por cuanto no había obligación para las operadoras de conservarlos, y si ellas llegaban a hacerlo era para finalidad de facturación, amparándose en el artículo 18 N°4 de la Constitución.[261]

El **artículo 1**, respecto de su ámbito de aplicación, dispone que se aplicará a la persecución de "delitos graves" contemplados en la legislación penal general o especial, esto es, serían aquellos previstos en el artículo 13 del Código Penal español, que incluye a aquellos que se castigan con pena grave. Esto nos dirige al artículo 33.2 del mismo cuerpo legal, que califica como tal las penas de prisión superior a 5 años.[262] Luego, el mismo artículo indica que se aplicará a los datos de tráfico y de localización de personas y datos relacionados que permitan identificar a un abonado o usuario.

El **artículo segundo** dispone que los obligados a la conservación de datos son los operadores de comunicaciones.

---

[261] RODRÍGUEZ LAINZ, JOSÉ LUÍS (2011) "Estudios sobre el secreto de las comunicaciones. Perspectiva doctrinal y jurisprudencial". España. Wolters Kluwer España, S.A. Disponible en línea en <http://www.digitaliapublishing.com.uchile.idm.oclc.org/visorepub/49177> [Visto en línea 18/11/2020].

[262] CABELLO GIL (2017) op. cit. p. 146.

El **artículo tercero** hace una pormenorizada enumeración de los datos sujetos a la obligación de conservación, que, según el preámbulo de la ley, "serían los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado", incluyendo telefonía por Internet.[263] A vía ejemplar, se incluye los números telefónicos involucrados o marcados, nombre y dirección del abonado o usuario; el IMSI, IMEI, tanto de quien efectúa llamada como de quien la recibe, el identificador de celda y la fecha y hora en que se haya activado el servicio con tarjetas prepago. Se incluyen además las llamadas infructuosas, según lo prescribe el artículo 4.2.

Especial importancia para nuestro trabajo tiene la letra f) del apartado primero:

> "f) Datos necesarios para identificar la localización del equipo de comunicación móvil:
>
> 1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.
>
> 2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones."

En cuanto al plazo de conservación, **el artículo 5** señala que debe ser como mínimo de 12 meses contados desde la fecha en que se genera la comunicación, luego de lo cual establece la posibilidad de ampliar o reducir el plazo de forma reglamentaria, fijando un rango de mínimo seis meses y hasta 2 años, teniendo en consideración el valor de almacenamiento, gravedad del ilícito, entre otras circunstancias.

En cuanto a la cesión de datos, el artículo sexto prevé que solo procede de acuerdo con los fines que esta ley establece y previa autorización judicial. Entre los agentes facultados para que les sean cedidos los datos se encuentra la policía judicial, que se encarga de combatir la delincuencia[264].

Finalmente, el capítulo III establece cuáles son las infracciones a las obligaciones de esta ley y las sanciones que conllevan, la que se rigen según la Ley General de Telecomunicaciones.

---

[263] Preámbulo Ley 25/2007 de 5 de octubre.

[264] Artículo 6.2 a).

b. Ley de Enjuiciamiento Criminal.

En la legislación española la localización por medio de la obtención de datos de una estación base se encuentra regulada en la Ley de Enjuiciamiento Criminal[265] (en adelante LECr.); la cual, desde una modificación realizada el año 2015 (L.O. 13/2015), prevé tales medios de prueba dentro del título referido a las medidas de investigación limitativas de derechos fundamentales reconocidos en el artículo 18 de la Constitución Española. (Libro I, Título VIII, Capítulo IV). Al respecto debemos considerar que la Constitución consagra los siguientes derechos:

"Artículo 18

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

b.1. Disposiciones Comunes.

En primer lugar, el capítulo IV, cuyo título es bastante extenso, regla las disposiciones comunes de las distintas medidas que entran en conflicto con el artículo 18 de la Constitución española, entre las que se encuentra el tratamiento de datos de tráfico.

b.2. Principios rectores (588 bis a)

En primer lugar, se establece que para realizar alguna de las medidas se requerirá de "autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida". Luego, se refiere a cada uno de los principios en particular:

[265] ESPAÑA. Ministerio de Gracia y Justicia (1882) *Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.* (17/09/1882).

1) **Principio de especialidad:** La medida debe estar relacionada con la investigación de un delito concreto, que tenga base objetiva.
2) **Principio de idoneidad:** Debe tomarse en cuenta la utilidad de la medida al momento de definir su ámbito objetivo y subjetivo y la duración de esta.
3) **Principio de necesidad y excepcionalidad de la medida:** Se requiere que no haya otra medida menos gravosa para los derechos fundamentales del investigado e igualmente útiles para la investigación; Debe verse gravemente dificultado el esclarecimiento del caso para que proceda la medida.
4) **Principio de proporcionalidad:** El sacrificio de los derechos e intereses afectados no es superior al beneficio que la adopción de la medida tiene para el interés público y terceros, teniéndose en consideración la gravedad del hecho, su trascendencia social, intensidad de los indicios existentes y la relevancia del resultado perseguido.

b.3. Duración de las medidas (588 bis e) y f).

Si bien el artículo 588 bis e) dispone que cada una de las medidas previstas, considera reglas especiales para la definición de su duración, prevé como regla general que las medidas no podrá exceder del tiempo imprescindible para el esclarecimiento de los hechos. Consecuente con lo anterior, se prevé la posibilidad de que la medida sea prorrogada, en la medida que subsistan las razones que la motivaron y se cumplan los requisitos que señala el artículo 588 bis f); esto es, en cuanto a la oportunidad, que se dirija por el Ministerio Fiscal o la Policía Judicial al juez competente con la debida antelación a la expiración del plazo inicialmente concedido y que la solicitud incluya el informe detallado del resultado de la medida, y las razones que justifiquen la mantención de la misma.

Sin perjuicio de lo anterior, el artículo 588 bis j), se refiere al **cese de la medida**, el que procede cuando “desaparezcan las circunstancias que justificaron su adopción” o cuando no se esté obteniendo los resultados esperados. Finalmente procede siempre por el transcurso del plazo.

b.4. Solicitud y Autorización Judicial.

En seguida los artículos 588 bis b) y 588 bis c) regulan la **solicitud de autorización y la resolución judicial** respectivamente, enumerando una lista de información y peticiones que debe contener cada una. La **solicitud** debe incluir las razones que justifiquen la necesidad de la medida; los indicios de criminalidad; extensión de la medida; su duración; el sujeto obligado que la llevará cabo; entre otras.

Respecto de **la autorización como tal,** esta deberá dictarse en un plazo máximo de 24 horas desde que se presenta la solicitud, a pesar de que se puede interrumpir ese plazo cuando el juez requiera de una aclaración de la solicitud.

En cuanto a su contenido, se destaca que debe ser fundamentada en conformidad a los principios rectores; la finalidad de la medida; su duración; la unidad policial encargada; el sujeto obligado, señalándole el deber de colaboración y de guardar secreto bajo apercibimiento de incurrir en delito de desobediencia.

b.5. Deber de secreto y destrucción de registros (588 bis d) y k).

El artículo 588 bis d) establece que tanto la solicitud como las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una **pieza separa y secreta**, sin necesidad de que se acuerde expresamente el secreto de la causa.

En cuanto a la **destrucción de registros,** según el artículo 588 bis k), es obligatoria cuando se ponga término al procedimiento mediante resolución firme, salvo por una copia que quedará bajo custodia del secretario del tribunal, que debe destruirse una vez que se esté frente a los supuestos del apartado 2°, esto es “cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, siempre que no fuera precisa su conservación a juicio del Tribunal”.

b.6. Disposiciones generales a la interceptación de las comunicaciones telefónicas y telemáticas.

El tratamiento de los datos de tráfico se regula en la Sección 2° del Capítulo V, denominada "Incorporación al proceso de datos electrónicos de tráfico o asociados". Dicho Capítulo V regula la "interceptación de las comunicaciones telefónicas y telemáticas".

Con anterioridad, en la sección 1°, se regulan las disposiciones generales entre las que se encuentran los presupuestos; el ámbito; la afectación a terceros; la solicitud de autorización judicial; deber de colaboración; control de la medida; duración; solicitud de prorroga; y el acceso de las partes a las grabaciones.

En cuanto a la **solicitud de autorización judicial**, indicando que debe contener la identificación del número del abonado, del terminal o de la etiqueta técnica; la identificación de la conexión objeto de la intervención; los datos necesarios para identificar el medio de telecomunicación; origen o destino; localización geográfica del origen o destino de la comunicación. En especial, para obtener los datos de tráfico, el artículo 588 ter d en el literal d) del párrafo 2 prescribe que debe especificarse los "datos concretos que han de ser obtenidos."

b.7.Tratamiento de datos de tráfico.

El inciso tercero del artículo 588 ter b.2, entrega una **definición de lo que debe entenderse por datos electrónicos de tráfico o asociados**, refiriéndose como tales a "todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicos, de su puesta a disposición del usuario, así de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga".[266]

Por su parte, el artículo 588 ter j), se encarga de normar **la incorporación al proceso de datos electrónicos de tráfico o asociados.** En él se dispone que éstos solo podrán ser entregados para incorporarlos al proceso cuando exista la debida autorización judicial, cualquiera sea la razón por la que los operadores los hayan conservado: bien por la obligación de conservación que impone la Ley 25/2007, bien por iniciativa propia por cualquier motivo. A su vez, el inciso

[266] ESPAÑA. Ministerio de Gracia y Justicia. 1882. *Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.* 14 de septiembre de 1882.

segundo del mismo artículo da la posibilidad de solicitar autorización del juez para recabar información que conste en archivos automatizados de los prestadores de servicios, incluyendo la búsqueda entrecruzada o inteligente de datos cuando el conocimiento de esos datos resulte indispensable para la investigación.

b.8. Acceso a datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.

La **sección tercera del capítulo** regula el acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, sea a través del número IP para el caso de delitos que se cometan a través de internet, o bien se trate de la identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes. En el segundo caso, la Policía Judicial puede valerse de medios técnicos que permitan conocer códigos de identificación o etiquetas técnicas del aparato, o bien su IMSI o IMEI cuando no hubiera sido posible obtener un determinado número de abonado indispensable en el marco de una investigación. Finalmente, el artículo 588 ter m). Regula la posibilidad del Ministerio Fiscal o Policía Judicial de solicitar a los operadores de telecomunicaciones que proporcionen información acerca de la titularidad de un número telefónico o del número como tal, o los datos identificativos de cualquier medio de comunicación.

b.9. Dispositivos o medios técnicos de localización (588 quinquies b).

Siempre que la medida sea necesaria y proporcional y el juez así lo autorice, el juez competente podrá autorizar la utilización de dispositivos o medios técnicos de seguimiento y localización.

Esta expresión incluye aquellos medios que pueden ser o venir instalados en determinados objetos y que permiten obtener información acerca de la ubicación geográfica de éstos, por ejemplo aquellos que pueden instalarse en automóviles, aquellos que vienen integrados en teléfonos móviles, como son el sistema GPS o los dispositivos de geolocalización que se instale en una prenda de ropa de una persona, por señalar algunos.[267]

[267] MAÑAS MARÍN, CRISTINA (2018) *La localización del sospechoso mediante dispositivos de seguimiento y su aplicación en el proceso penal. Prueba ilícita.* Trabajo de grado de Derecho. Colegio Universitario de Estudios Financieros, p. 8.

La norma señala que la resolución respectiva deberá especificar el medio técnico a utilizar. Asimismo, impone la obligación de los operadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, y otros a colaborar con los órganos investigativos para llevar a cabo esta medida.

De manera complementaria, la **Circular 4/2019 de la Fiscal General del Estado**, sobre utilización de dispositivos técnico de captación de la imagen, de seguimiento y localización, establece que se requiere autorización judicial debido a que "supone una limitación al derecho de intimidad de la persona, pero no de su derecho al secreto de las comunicaciones".[268] Se trataría de una "limitación de baja intensidad".[269] La circular además indica que la geolocalización es aplicable "únicamente a la obtención de datos de geolocalización en tiempo real"[270], sea través dispositivos abiertos o cerrados y automatizados.

Asimismo, la Circular nos recuerda que la autorización de la medida debe tener en consideración los principios rectores de los artículos 588 bis a) y siguientes, haciendo presente que existe una "menor intensidad en la intromisión de derechos fundamentales" y ello debe tener su correlato en la severidad de la aplicación de los principios.[271]

c. Ley General de Telecomunicaciones de 2014.

La 9/2014, Ley General de Telecomunicaciones[272], publicada el 9 de mayo de 2014, la que, en lo que nos interesa, regula el secreto de las comunicaciones y protección de los datos personales en su capítulo III.

---

[268] ESPAÑA. Ministerio Fiscal. (2019) *Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización.* Boletín Oficial del Estado N° 70, de 22 de marzo de 2019. p. 30157.

[269] Ibid.

[270] Ibid. En los casos que se trate de geolocalización de comunicaciones ya acontecidas, ella se regirá por el artículo 588 ter j o 588 sexies a, según si se trata de datos asociados a comunicaciones telefónicas o datos almacenados en dispositivos GPS hallados en poder del investigado.

[271] Ibid. 30.158.

[272] ESPAÑA. Jefatura de Estado (2014) *Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.*

A propósito del **secreto de las comunicaciones**, el artículo 39 regula extensamente la interceptación de las comunicaciones; donde se impone a los sujetos obligados facilitar los datos o "información relativa a la interceptación" que el artículo 39.5 enumera (salvo que por las características del servicio tales datos no estén a su disposición), entre los que se encuentra la información de localización (literal i). Junto con esto el **apartado 7** establece la obligación de proporcionar la "situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada", como asimismo "una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada, salvo que por las características del servicio no los tengan a disposición."

Si estos datos de localización forman parte de la comunicación como tal, como sería el caso una persona que comparte su ubicación vía WhatsApp, se encontrarían protegidos por el secreto de las comunicaciones.[273]

El artículo 42, por su parte, se encarga de la **conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones**, remitiéndose a la Ley 25/2007, de 18 de octubre.

d. Breve mención de la Ley Orgánica de Protección de Datos Personales de 2018.

El 5 de diciembre de 2018 se publicó la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales[274], que reemplazó a su predecesora de 1999, LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. La ley, cuyo objeto es "garantizar los derechos digitales de la ciudadanía" en virtud del derecho a la protección de datos personales",[275] adecúa la normativa interna al Reglamento (UE) 2016/679 del Parlamento Europeo y Consejo, sobre protección de datos, así como marco de aplicación de la protección de los datos personales regulada en el artículo 18.4 de la Constitución Española.

Con todo, no analizaremos en detalle sus contenidos porque esta ley no es aplicable al tratamiento de datos "por parte de las autoridades competentes con fines de prevención,

[273] CABELLO GIL (2017) op. cit. p 151-152.

[274] ESPAÑA. Jefatura de Estado (2018) *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.* 5 de diciembre de 2018.

[275] Artículo 1.3.

investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales incluida la de protección frente a amenazas a la seguridad pública y su prevención".[276] Esto es así por la remisión que el artículo 2.2 de la ley hace al artículo 2.2 del Reglamento 2016/679 del Parlamento Europeo y Consejo.

e. Datos de Tráfico y Derechos Fundamentales en España.

José Julio **Fernández** Rodríguez, de la Universidad de Santiago de Compostela, se refiere a la relevancia que tiene la seguridad en el desarrollo de una "adecuada calidad democrática"[277]. Al respecto señala que el concepto seguridad incluye tanto la seguridad nacional, o seguridad del Estado- como la seguridad pública o ciudadana, que se refiere a la persecución de delitos. En palabras de este autor, la variedad de información que compone los datos de tráfico, "tanto de forma aislada, pero sobre todo en conjunto, revelan aspectos de la vida privada y la intimidad. Quién se ha comunicado con quién, con qué frecuencia, en qué momento y de qué modo",[278] pudiendo así quedar al descubierto hábitos y tendencias de las personas. Asimismo, contienen datos personales, puesto que a partir de algunos de ellos se puede hacer identificable a una persona, corriéndose el riesgo de provocar una autocensura generalizada de la población.[279]

En este sentido es que el autor concluye que "los metadatos afectan al derecho a la intimidad […] y la libertad de expresión […]".[280] Asimismo, cuando a partir de ellos pueda llegarse a identificar a una persona, se afecta el derecho a la protección de datos. Y cuando, a través de GPS, es posible dar con la ubicación de una persona, se estaría también afectando el derecho a la libre circulación; todos derechos consagrados en la Constitución española.[281]

---

[276] UNIÓN EUROPEA. Parlamento Europeo y Consejo (2016*) REGLAMENTO (UE) 2016/679 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).* Art. 2.2.

[277] FERNÁNDEZ, JOSÉ JULIO (2016) *Los datos de trafico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente.* Revista Española de Derecho Constitucional N° 108, 93-122, p. 97.

[278] Ibid., p. 99.

[279] Ibid.

[280] Ibid., p. 100.

[281] Ibid.

Ahora bien, una cuestión sustancial que se plantea dice relación con si la utilización de datos de tráfico implica o no una afectación del derecho al secreto de las comunicaciones[282] En este sentido, se plantea que, si bien la medida no involucra conocer el contenido del mensaje, llamada o, en general, comunicación, sí se estaría vulnerando, toda vez que es posible dar con la identidad de los comunicantes a partir del conocimiento de las terminales de los interlocutores. Así, se sostiene que "la conservación también afecta al secreto de las comunicaciones."[283]

En el mismo sentido se ha pronunciado el tribunal constitucional español, aunque reconociendo que la injerencia es de "menor intensidad cuando no se accede al contenido".[284]

Junto con ello, se sostiene que "en el tema de los datos de tráfico están presentes dos de los argumentos de fondo que sostienen las garantías del secreto de las comunicaciones: estos datos se ubican en **canal cerrado** y sobre ello el emisor tiene **expectativa de privacidad".**[285]

Entonces, la calificación jurídica del dato va a depender de cada uno de ellos en particular. Así, en definitiva, los datos que entreguen la identidad de los interlocutores afectan el derecho al secreto de las comunicaciones, es decir a la inviolabilidad de ellas. Por el contrario, cuando estemos frente a datos de tráfico tales como la duración de la llamada o la localización de los interlocutores, existirá una afección a la intimidad, la protección de datos o la libertad de circulación.[286]

Con respecto a la conservación de los datos, ello tiene justificación siempre para efectos de facturación de las empresas de telecomunicaciones, en el sentido de que la información conservada sirva para efectos de saber qué y cuánto cobrar a los clientes. Tanto es así que, en el contrato entre la empresa operadora y el potencial cliente, se hace, por lo general, mención acerca de la conservación de datos para efectos de realizar la facturación respectiva.

Otra razón por la que se justifica la conservación de datos se refiere a la protección de la seguridad, sea nacional o pública. En tal sentido, se ha dicho que "los datos conservados son

[282] Artículo 18.3 de la Constitución española.

[283] Ibid. p. 101.

[284] Ibid. SSTC 114/1984, FJ7 7; 123/2002, FJ 5-6; 56/2003, FJ 2; 230/2007, FJ 2-3.

[285] Ibid.., p.102.

[286] Ibid.

valiosos para los enjuiciamientos e investigaciones penales al permitir establecer pistas sobre un delito, excluir a sospechosos, confirmar coartadas, contactar con testigos o iniciar investigaciones penales".[287]

Prueba ilícita en España

La protección de los derechos fundamentales se plasma en el concepto de **prueba ilícita**; esto es, la obtenida de manera ilegal o vulnerando los derechos fundamentales protegidos por la constitución.[288] En efecto, se debe tener en consideración **el principio de legalidad de la prueba**, que exige que las evidencias se obtengan e incorporen al proceso de conformidad con los principios y disposiciones legales.[289] Asimismo, debe tenerse en cuenta el **principio de licitud de la prueba**, que exige que toda evidencia respete los derechos fundamentales. [290]

Se vulneran estos principios cuando, por ejemplo, la prueba es obtenida vulnerando derechos fundamentales, o que no ha sido conservada de manera óptima [cadena de custodia], o porque la ley procesal no permite determinado medio de prueba o forma de presentarlo, lo que la jurisprudencia española llama "prueba irregular".[291]

3. Jurisprudencia Española acerca de la prueba indiciaria: Tribunal Supremo, Sentencia 100/2019.

Como ya hemos planteado con anterioridad en esta investigación, la localización de un sospechoso en las proximidades del sitio del suceso en el momento que este ocurre no es un hecho directo que, de por sí, permita acreditar la culpabilidad de un sospechoso respecto de un delito perpetrado. No obstante, es posible ofrecerla en el proceso en calidad de indicio -también conocido como hecho base-. Pero para que los indicios puedan tenerse en consideración por el juez, deben cumplirse tanto requisitos formales como materiales. La sentencia que estudiaremos

[287] Ibid. P. 104.

[288] MAÑAS MARÍN (2018) op. Cit., p. 33.

[289] Ibid., p. 34.

[290] Ibid.

[291] Ibid., p. 35.

a continuación nos ilustra acerca de los indicios y su validez como medio probatorio según las explicaciones de las máximas autoridades judiciales en España.

El 26 de febrero de 2019, la Sala de lo Penal del Tribunal Supremo de España, a través de la sentencia 100/2019,[292] desestimó un recurso de casación por infracción de ley e infracción del precepto constitucional que impetró quien fuera declarado culpable en primera y segunda instancia de un delito de femicidio con alevosía en contra de su expareja. El precepto constitucional que se planteaba vulnerado fue el derecho de presunción de inocencia, toda vez que, señalaba el recurrente, la prueba rendida en su oportunidad no permitía dar por acreditado que este asesinara a su expareja. Por esta misma razón se adujo que existía vulneración del principio pro-reo y la teoría de la duda razonable.[293]

Y es que dentro de dichas probanzas se encontraban solamente indicios, de diversa índole, por ejemplo, relatos de testigos que oyeron gritos desde el departamento de la víctima durante la madrugada; piel del malhechor en las uñas de esta; y -lo que más nos interesa- prueba de geolocalización que permitió acreditar que el imputado no se encontraba donde declaró haber estado las horas después del suceso. Más aún, dicha localización fue posible debido a las llamadas realizadas y recibidas desde el teléfono de la víctima con posterioridad a su muerte, que lo ubicaban en un lugar distinto del sitio del suceso, pero a su vez distinto del que él había declarado estar. El jurado en primera instancia estimó que el hombre se había llevado consigo el teléfono móvil de la víctima una vez que la asesinó.

También fue considerado el hecho base de que el malhechor conocía a la víctima, puesto que una testigo declaró que escuchó a la víctima gritar “cómo me haces esto a mí”; además de que la víctima temía a su expareja, conclusión a que llegó el jurado por el hecho de haber cambiado la cerradura de la puerta de acceso a su domicilio pocos días antes del suceso. Ambos constituyen indicios de la responsabilidad de este hombre. Aun así, el jurado estimó que este entró con llaves o le abrieron la puerta, ya que no había signos de haberse forzado.[294]

[292] TRIBUNAL SUPREMO DE ESPAÑA, Sala de lo Penal (2019) Sentencia número 100/2019.

[293] Ibid., p. 8.

[294] Ibid., p. 12.

Del mismo modo, se acreditó que la víctima sentía temor del hombre; que la relación afectiva entre ambos estaba seriamente dañada; que el recurrente buscó asegurar que la víctima estuviera sola; la desaparición de la ropa que el recurrente llevaba ese día según constaba a través de material audiovisual; entre varias otras.[295]

En cuanto a la geolocalización, los técnicos determinaron lo siguiente: "a las 3.39 horas del día 1 de noviembre de 2014 uno de los teléfonos de Leonardo estaba conectado a la celda 29757 bajo la antena que da cobertura tanto al domicilio de él como de la víctima. Y permaneció bajo esa misma cobertura durante 2 horas y 39 minutos, por lo que pudo desplazarse al domicilio de R. sin salto de celda o cobertura".[296]

La sentencia se pronunció respecto de cuáles son las condiciones que deben existir para que el indicio sea suficiente para enervar el principio de inocencia.

Así, señala qué la prueba indiciaria se utiliza en "casos en los que no existe prueba directa y es preciso acudir al enlace preciso y directo que proporcionan sucesivos indicios que debidamente concatenados dan lugar a la existencia de una prueba tenida como 'de cargo' por el Tribunal y que es admitida para enervar la presunción de inocencia".[297]

El fallo hace referencia de diversos pronunciamientos que dicho Tribunal ha hecho sobre la validez de la prueba indiciaria, mencionando que "supone un **proceso intelectual complejo** que reconstruye un hecho concreto a partir de una recolección de indicios",[298] de manera que, constatándose hechos mediatos, estos permitan llegar a concluir hechos inmediatos.

De todas maneras, el Tribunal señala que ha de **expresarse claramente la "hilazón [sic] lógica** de los indicios sobre los que se construye la decisión", de forma tal que el proceso deductivo quede plasmado, para así permitir hacer un "control de la racionalidad del hilo discursivo". Así debe "quedar al descubierto el juicio de inferencia como actividad intelectual que sirve de enlace a un hecho acreditado y su consecuencia lógica".[299]

---

[295] Ibid., p. 13- 22.

[296] Ibid., p. 17.

[297] Ibid., p. 32.

[298] Ibid.

[299] Ibid.

A continuación el fallo aclara que la acreditación de hechos **mediante indicios no obsta al principio de presunción de inocencia**, siempre que se cumpla con los **requisitos** de que (1) tales indicios estén "plenamente acreditados", siendo insuficientes las meras sospechas; (2) que quede explicito en el fallo el razonamiento a través de cual el órgano jurisdiccional "ha llegado a la convicción sobre el acaecimiento del hecho punible y la participación en el mismo del acusado", que se condiga con las reglas de la lógica y la experiencia y criterio humano.[300] De forma tal que, de ser ciertos los indicios, haya de serlo también el "hecho determinante de la culpabilidad".

El Tribunal Supremo cita un fallo de este, que hace una **profunda e interesante reflexión** acerca de los indicios:

"[N]acen las presunciones e indicios del conocimiento de la naturaleza humana, del modo de comportarse habitual del hombre en sus relaciones con otros miembros de la sociedad, de la índole misma de las cosas. La importancia de la prueba indiciaria en el procedimiento penal radica en que, en muy varios supuestos, es el único medio de llegar al esclarecimiento de un hecho delictuoso y al descubrimiento de sus autores".[301]

Más adelante se refiere a **los requisitos formales y materiales** que la jurisprudencia ha exigido para la validez de los indicios:

Los **requisitos formale**s son (**1**) que la sentencia exprese cuales son los indicios que se estiman acreditados y que serán fundamento a la inferencia; y (**2**) que en la sentencia se encuentre explícito el razonamiento lógico que permite, a través de los indicios, llegar a la convicción del "acaecimiento del hecho punible y la participación del acusado en el mismo". De esta manera se permite el "control casacional de la racionalidad de la inferencia".[302]

En cuanto a los **requisitos materiales**, hay que subdividir en los que respectan a los indicios como tales y, por otro lado, a la deducción o inferencia.

En lo **referente a los indicios**, la sentencia establece que **(1)** deben estar plenamente acreditados; **(2)** que sean múltiples, o excepcionalmente único, pero con "singular potencia";

[300] Sentencia 1980/2000 25/01/2001. Citada en: Ibid., p.32.

[301] Sentencia 913/1996, de 26 nov. Citada en: Ibid., p. 33.

[302] Ibid., p. 34.

(3) que sea concomitantes al hecho que se trata de probar; y **(4) "**que exista interrelación entre los varios indicios, de manera que se refuercen entre sí".[303]

Ahora respecto a **la inducción o inferencia**, debe ser **razonable**, esto es "que responda plenamente a las reglas de la lógica y de la experiencia, de manera que de los hechos base acreditados fluya, como conclusión natural, el dato precisado de acreditar, existiendo entre ambos un 'enlace preciso y directo según las reglas del criterio humano'."[304]

Por otro lado, el TC español establece como requisitos "imprescindibles para que opere la prueba indiciaria", **(1)** que los indicios estén plenamente probados; **(2)** "que los hechos constitutivos del delito deben deducirse precisamente de estos hechos base completamente probados"; **(3)** que el tribunal exteriorice los hechos que están acreditados y el razonamiento o "engarce lógico" entre los "hechos-base y los hechos-consecuencia"; y **(4)** que el razonamiento esté asentado en las reglas de la experiencia común.[305]

En definitiva, se requiere que los indicios mantengan una correlación que permita arribar a una determinada convicción, a través del uso de razonamiento lógico.

4. Marco Jurídico Peruano.

Con fecha 27 de julio de 2015 fue publicado el llamado "Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado", con el cual se pretendía poner término al aumento de la criminalidad que venía aconteciendo en el Perú durante los últimos años.[306]

Esta normativa faculta a la policía para realizar diligencias de geolocalización.

En lo que respecta a derechos fundamentales, el decreto, si bien fue desarrollado con la intención de que no tuviera vulneración alguna de éstos (artículo 6°), la verdad es que, como señala

[303] Ibid., p. 34.

[304] Ibid., p. 36.

[305] Ibid.

[306] ELÍAS PUELLES, RICARDO (2016) *Decreto Legislativo 1182, Geolocalización y Proceso Penal.* Lima, Perú, Hiperderecho. P.7.

Ricardo **Elías Puelles**, en efecto sí lo hace. Esto es, según él, porque las diligencias requieren de una audiencia de convalidación, posterior al ejercicio de la diligencia por parte de la policía, con lo que, indirectamente, se reconoce que se están afectando derechos fundamentales.[307]

Así, el mismo autor sostiene que "con las nuevas tecnologías lo que se transmite no sólo es el contenido (mensaje) sino también información relacionada al emisor sea de manera consciente o inconsciente".[308] Con todo, la vulneración de derechos fundamentales no es tan grave como lo es en casos de intervenciones telefónicas.

Por otro lado, sostiene el autor que existe una afectación al derecho de intimidad "por cuanto todas las personas tienen el derecho de defenderse de la divulgación de hechos privados".[309] En este sentido señala que este decreto "no solo permite localizarnos en tiempo real sino acceder a nuestra localización histórica y monitorear nuestro desplazamiento futuro".[310]

En Perú existe una garantía fundamental conocida como Derecho a la Autodeterminación Informativa, que consiste en que es derecho de los titulares de determinada información la toma de decisión de entregar o no ésta. En este sentido, se estaría afectando tal derecho, toda vez que "deberían ser los titulares de las líneas telefónicas quienes autoricen la ubicación de sus equipos telefónicos o, en todo caso, el juez a través de una resolución debidamente motivada".[311]

En cuanto a qué gravedad debiera tener una infracción para ser susceptible de aplicación de medidas de geolocalización por parte de la policía, el decreto legislativo indica que procede en casos de flagrancia delictiva, como también cuando se trata de delitos que tengan como pena una mayor a cuatro años, siempre que exista una necesidad, en su sentido doctrinario, para llevarse a cabo la medida.

En lo que se refiere a casos de flagrancia, este autor sostiene que "es imposible jurídicamente que nos encontremos ante supuestos de flagrancia que habiliten la geolocalización del presunto agente, ya que dicha figura requiere dos elementos: inmediatez temporal e inmediatez

[307] Ibid p. 9.

[308] Ibid.

[309] Ibid.

[310] Ibid.

[311] Ibid.

personal".[312] Esto sería así porque el elemento de **inmediatez personal** no concurre en estos casos, en que los "delitos son cometidos a través de dispositivos móviles o similares".[313]

En cuanto al requisito de que la medida sea **necesaria,** dentro de un estudio de la proporcionalidad de la medida, tal estimación queda en manos de la Policía, y no de un Fiscal. Entonces se "propicia la confusión jurídica de roles"[314] al permitir que sea aquélla la que evalúe si existe o no la necesidad de llevar a cabo la medida.

Por su parte, es interesante señalar que, "en vez de seleccionar un grupo específico de delitos en los que se podría aplicar la geolocalización, como en el caso de la interferencia de las comunicaciones, el Ejecutivo aprobó que sea aplicable a todos los ilícitos sancionados con pena superior a cuatro años de privación de libertad".[315] Por ende, la aplicación de la geolocalización no solo procede respecto de delitos calificados como graves, lo que, en palabras de Elías, "posibilita la ubicación en tiempo real de cualquier ciudadano que cuente con un dispositivo electrónico y que haya sido denunciado ante la Policía";[316] lo cual significaría una afectación no menor al derecho a la intimidad, consagrado en la Constitución Política del Perú.

Ricardo Elías hace un resumen del procedimiento que establece el Decreto Ley en cuestión para efectos de realizar la geolocalización. En definitiva, el primer paso lo da la unidad a cargo de la investigación policial, poniendo en conocimiento al Ministerio Público el hecho y formulando luego un requerimiento a la "unidad especializada de la Policía Nacional del Perú para efectos de la localización o geolocalización".[317]

A continuación, el Decreto Ley dispone que "la unidad especializada de la Policía Nacional del Perú que recibe el requerimiento, previa verificación del responsable de la unidad solicitante cursa el pedido a los concesionarios de los servicios públicos de telecomunicaciones o a entidades públicas relacionadas con este servicio, a través del correo electrónico institucional u otro medio idóneo convenido".

---

[312] Ibid. p. 10.

[313] Idem.

[314] Ibid.

[315] Ibid. p. 12.

[316] Ibid.

[317] Ibid. p. 13.

Pero a este respecto el autor sostiene que la Policía no posee la prerrogativa constitucional para solicitar datos de localización o geolocalización a las empresas mencionadas, puesto que existe una protección fruto del derecho fundamental de secreto de las comunicaciones. Según Elías toda la cadena de comunicación debe encontrarse en la carpeta o expediente fiscal, pues de lo contrario se estaría frente a una restricción del derecho a la defensa.[318]

Otro tema interesante que dispone la ley en cuestión se encuentra en su artículo 4, inciso tercero, que señala que los concesionarios o servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, están obligados a brindar los datos de localización o geolocalización de manera inmediata, las veinticuatro (24) horas del día de los trescientos sesenta y cinco (365) días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento.

Continuando con el procedimiento, el artículo 5.2 prescribe que la unidad policial a cargo de la investigación policial, dentro de las 24 horas de comunicado el hecho al Fiscal correspondiente, le remitirá un informe que sustente el requerimiento para su convalidación judicial (artículo 5.1). El Fiscal dentro de las veinticuatro (24) horas de recibido el informe, solicita al Juez la convalidación de la medida. En cuanto a esto, Elías sostiene que "si el Fiscal no está de acuerdo con la solicitud de la Policía tiene toda la potestad de ordenar se deje sin efecto la medida".[319]

El siguiente paso en el procedimiento, es el que dice relación con que el juez competente debe dictar resolución en un plazo no mayor a 24 horas. Resulta que se trata de una convalidación judicial de la medida de geolocalización una vez que fue efectuada y, lamentablemente, no un control judicial previo, que permita que se indique expresamente la información que la Fiscalía requiere, con tal de evitar una vulneración al derecho a la intimidad.[320]

El autor recalca que el Decreto Ley no se hace cargo del caso en que se acuda directamente ante el Ministerio Público para efectos de denunciar un ilícito, dejando abierta la posibilidad de que deba de comunicarse con la Policía para efectos de efectuar la medida; con lo que se estaría

[318] Ibid.

[319] Ibid. p. 14.

[320] Ibid. p. 15.

frente a un procedimiento “monopolizado por el Ejecutivo, a través de la Policía, desplazando a su vez al titular natural de la acción penal”.[321]

Según las propias palabras del autor en análisis “el Decreto Legislativo le confiere el carácter de jurisdiccionalidad a un acto policial. Este hecho vulnera el numeral 3 del artículo IV del Código Procesal, el cual prevé que los actos de investigación que practica el Ministerio Público o la Policía Nacional no tienen carácter jurisdiccional, (...) se requiere de autorización judicial previa para acceder a los datos de localización y geolocalización de dispositivos móviles por cuanto estos pertenecen a un titular (a una persona) cuyos derechos al secreto de las comunicaciones, a la intimidad y a la autodeterminación informativa se encuentran protegidos constitucionalmente”.[322]

De esta manera, se concluye que la actuación policial es ilegal, ya que las medidas que afectan derechos fundamentales requieren de autorización judicial previa, motivada y con estricto respeto del principio de proporcionalidad.[323]

Por otra parte, “los medios de prueba obtenidos a través del Decreto Legislativo generan prueba prohibida”.[324] Esto sería así como consecuencia de lo señalado en el párrafo anterior. El artículo VIII del Código Procesal Penal peruano permite llegar a tal conclusión.

[321] Ibid. p. 16.

[322] Ibid. p. 17.

[323] Ibid. p. 18.

[324] Ibid.

Conclusiones.

> Si un hombre acusa a otro hombre y le imputa un asesinato, pero no puede probarlo, su acusador será ejecutado.
>
> Parágrafo 1, Código de Hammurabi.[325]

Inserto estas palabras para, de forma simbólica, ilustrar lo fundamental que fue y sigue siendo la prueba de los hechos dentro del proceso judicial. Y es en atención a esta imprescindibilidad que se hace necesario recurrir a la mayor cantidad de evidencias posibles, a fin de asegurar el resultado del juicio; más aún en sede penal, en donde para enervar el principio de inocencia, el juez debe contar con una convicción más allá de toda duda razonable.

A través de este trabajo se pudo completar el objetivo de **fijar las bases metodológicas de la recogida, conservación y presentación en juicio, como prueba de la participación de un sujeto en un delito, de los datos de georreferenciación de dispositivos móviles,** lo cual puede sintetizarse en base a los resultados de cada uno de los objetivos específicos:

1.- En cuanto a **los conceptos técnicos básicos referentes a las telecomunicaciones,** logramos aprehender el concepto de "**datos de tráfico**", pese a la falta de definición en la legislación interna. exponiéndose cada una de las fases que implica, de manera de que a futuro pueda reproducirse la técnica eficazmente todos los involucrados en el proceso.

   Es así como si atendemos al convenio de Budapest, entendemos que los datos de tráfico, es un concepto genérico que incluye "todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente" (art. 1° letra d). Coincidimos con Fernández Rodríguez en cuanto a que este tipo de datos "son los datos que

[325] ANÓNIMO (s/f) *Código de Hammurabi* [en línea] Edición Luarna. Disponible en < http://www.ataun.eus/BIBLIOTECAGRATUITA/Cl%C3%A1sicos%20en%20Espa%C3%B1ol/An%C3%B3nimo/C%C3%B3digo%20de%20Hammurabi.pdf> [Visto en línea 10/05/2021].

rodean el mensaje que se transmite, pero que no forman parte de dicho mensaje" [326], son datos exactos, datos matemáticos, nítidos y fáciles de analizar.

Consistente con lo anterior, el proyecto de ley que se tramita en el Congreso Nacional, que busca adecuar la legislación nacional a los compromisos del Convenio de Budapest, los define en los siguientes términos: "entenderá por datos relativos a tráfico, todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, la localización del punto de acceso a la red, el destino, la ruta, la hora, la fecha, el tamaño y duración de la comunicación o el tipo de servicio subyacente".[327]

Un segundo concepto esencial para el método que estamos analizando es el de **Estación base** entendida como el "[c]onjunto de uno o más emisores o receptores de radio, o una combinación de emisores y de receptores incluyendo los equipos asociados, que permite, en un emplazamiento dado, asegurar un servicio de radiocomunicación o de radioastronomía".[328] Básicamente, es una "[i]nstalación destinada a proporcionar acceso al sistema de telecomunicaciones por medio de ondas de radio".[329] Cada estación base cubre una celda, por consiguiente, un conjunto de estaciones bases conforman las llamadas redes de celdas o redes celulares, que proporcionan cobertura de radio en áreas geográficas más extensas. Por lo tanto, el equipo de usuario (UE), como los teléfonos móviles, puede comunicarse incluso si el equipo se mueve a través de las células durante la transmisión" [330]

El tercer concepto esencial es el de **celda**, porque "En su operación, el teléfono móvil establece comunicación con una estación base y, a medida que se traslada, los sistemas computacionales que administran la red van transmitiendo la llamada a la siguiente estación

---

[326] FERNÁNDEZ, JOSÉ JULIO (2016) Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente. Revista Española de Derecho Constitucional, volumen 108 (p. 93- 122), p. 96.

[327] Artículo 14 del proyecto de ley.

[328] REAL ACADEMIA DE INGENIERÍA DE ESPAÑA (s/f) *Diccionario español de ingeniería: op. Cit.*

[329] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (2021) T*raducción libre del texto: "Installation intended to provide access to the telecommunication system by means of radio waves." ITU-T, K.56 (05/2021), Series K: Protection against interference. Protection of radio base stations against lightning discharches*". Disponible en línea en https://www.itu.int/rec/T-REC-K.56-202105-I/es, [Visto en línea 15/11/2021].

[330] TECHOPEDIA (s/f) *¿Qué significa red celular?* [en línea] https://www.techopedia.com/definition/24962/cellular-network [Visto en línea 17/11/2021].

base de forma transparente para el usuario. Por eso se dice que las estaciones base forman una red de celdas, sirviendo cada estación base a los equipos móviles que se encuentran en su celda".[331] En este contexto podemos definir como celda el territorio al cual da servicios una determinada estación base.

Finalmente, georreferenciación, deriva de georreferencial, "Que hace referencia a una zona geográfica específica dentro de la cual se recogen datos u otro tipo de información"[332]. Al respecto, la Defensoría Penal Pública hace referencia a esta expresión en los siguientes términos, relevantes al objeto de nuestro estudio, la "geolocalización de teléfonos celulares es un tipo de peritaje que permite establecer la ubicación geográfica de un *smartphone* al momento de realizar llamadas, enviar mensajes de texto o hacer uso de la red de datos"[333]

1. **Las metodologías y técnicas asociadas a la georreferenciación o geoposicionamiento de dispositivos móviles**,

2. Los **capítulos II y III, sobre el tratamiento de datos de tráfico con finalidades de investigación y garantías fundamentales**, nos permite adicionar al esfuerzo metodológico que hemos emprendido en este trabajo, los principios del debido proceso que deben tenerse en cuenta en la adopción de la técnica de geolocalización de equipos celulares dentro de un proceso penal. Al respecto, cobra especial relevancia que el derecho al secreto de las comunicaciones privadas, garantizado constitucionalmente no se vería afectado porque la técnica propuesta no representa una interceptación o escucha de la comunicación sino el posicionamiento del aparato terminal en determinada celda de la red celular.

Situación diferente es la del derecho a la protección de datos personales, por cuanto este método sí incluye el tratamiento de los datos del titular del aparato de que se trate. Asimismo, las

---

[331] RAMIREZ ZARATE, GUIMER (2014) *Implementación de seguridad domiciliaria mediante comandos AT sobre la tecnología de telefonía móvil.* Memoria para optar al grado de licenciado en electrónica y telecomunicaciones, Facultad de Tecnología Universidad Mayor de San Andrés, Bolivia. p. 14 [en línea] https://repositorio.umsa.bo/xmlui/bitstream/handle/123456789/11564/EG-1369-Ramirez%20Zarate%2C%20Guimer.pdf?sequence=1&isAllowed=y [Visto en línea 18/11/2021].

[332] Reglamento (CE) n.º 2152/2003 del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, sobre el seguimiento de los bosques y de las interacciones medioambientales en la Comunidad, art. 3."

[333] https://www.dpp.cl/sala_prensa/noticias_detalle/11489/defensoras-y-defensores-publicos-se-capacitan-en-geolocalizacion-y-georreferenciacion. [Visto en línea 11/03/2022].

garantías procesales, tales como el principio de inocencia, el derecho a defensa en juicio y el derecho a la prueba. Siendo así, se concluye que la inclusión de estas medidas requiere control judicial, proporcionalidad, y auditabilidad. Adicionalmente, consideramos que este tipo de pruebas no podría dar lugar a plena convicción sino que constituiría un indicio que se debe complementar con otros medios de prueba que se hayan rendido en el proceso.

3. Luego el capítulo IV, sobre **derecho comparado**, nos permitió analizar con mayor perspectiva la regulación extranjera sobre el tratamiento de datos de tráfico, con la finalidad de que pueda ser considerada en Chile, bien sea legislando en una línea similar, o bien, considerándola en la práctica por todos aquellos que participan en el proceso. A partir de ello hemos concluido la insuficiencia de nuestro marco normativo, puesto que, tratándose de medidas que afectan derechos fundamentales, no cabe la interpretación extensiva de las pocas normas que identificamos en nuestra normativa interna. Asimismo, si bien el proyecto de ley de adecuación de nuestra legislación al convenio de Budapest, de aprobarse aportaría una base conceptual mínima, es muy necesario que la legislación procesal penal desarrolle de manera exhaustiva esta materia.

4. Finalmente, en cuanto al **estándar procedimental que oriente la labor de los órganos de investigación y tribunales en las distintas fases, tanto recogida como conservación y presentación en juicio de estas pruebas**, atendido que el ordenamiento jurídico chileno carece de una regulación adecuada del tratamiento de los datos de tráfico para incorporarse como prueba en un proceso penal. Incluso, al estudiar los contenidos de los proyectos de ley hoy pendientes de aprobar, se puede notar que hay vacíos. Por ejemplo, no se regula un tiempo mínimo de conservación de datos por parte de las empresas de telecomunicaciones. Sin embargo, se aprecia en tales proyectos el interés por que estas medidas investigativas se realicen de la manera más expedita posible, al referirse al plazo que el juez impone en su autorización conducente a la entrega la información por parte de las empresas de telecomunicaciones. De todas maneras, habrá que esperar para ver cuál será el resultado final de dichos proyectos.

Se espera que este trabajo sea útil a la hora de llevar a cabo una investigación por parte del Ministerio Público; y para comprender la importancia de las limitaciones que implica la vulneración de diversos derechos fundamentales, y, en particular, el derecho a la protección de datos personales incorporado en nuestra Constitución Política hace algunos años. De esta forma

se recomienda tenerlo en consideración, para evitar futuros inconvenientes respecto de la prueba ilícita, la exclusión de la prueba o la declaración de nulidad de la sentencia, ambos por su inobservancia de las garantías fundamentales.

A su vez, se espera que el estudio del derecho comparado permita propagar el desarrollo de investigaciones que puedan servir al momento de proponer a las autoridades normativa adecuada respecto de esta materia en particular.

Urge una regulación más detallada para la recolección de datos de tráfico, que incluya una definición clara del concepto, una lista de los datos específicos que pueden recolectarse, tiempos mínimos y máximo de conservación por parte de las empresas de telecomunicaciones y otras entidades que se especifiquen, cadena de custodia, procedimiento a seguir por parte de las distintas entidades, entre otras.

Bibliografía

a. Doctrina

- 24 HORAS (2018) A*nalizarán tráfico de llamadas de sector donde murió Camilo Catrillanca* [en línea] <https://www.24horas.cl/nacional/analizaran-trafico-de-llamadas-de-sector-donde-murio-camilo-catrillanca--2883921> [Visto en línea 20/10/2019]
- ACCATINO, DANIELA (2011) *Certezas, dudas y propuestas en torno al estándar de la prueba penal.* Revista de Derecho de la Pontificia Universidad Católica de Valparaíso XXXVII [pp-483-511]
- ACCESS NOW. 2019. *Marianne Díaz Hernández elegida "Heroína" por su lucha contra la vigilancia y la censura del gobierno de Maduro* [en línea]. Accessnow.org. 8 de junio de 2019 <https://www.accessnow.org/marianne-diaz-hernandez-human-rights-hero-es/> [Visto en línea 3/12/2019]
- ALESSANDRI, A.; SOMARRIVA, M. & VODANOVIC, A. (1998) *Tratado de Derecho Civil. Tomo II.* Santiago de Chile: Editorial Jurídica de Chile
- ALLAN POE, EDGAR (2010) *Narraciones Extraordinarias*. Santiago de Chile: Zig-zag
- ALVARADO VELLOSO, ADOLFO (2009) *Sistema procesal, Santa Fe*, Argentina: Rubinzal-Culzoni editores
- ÁLVAREZ VALENZUELA, DANIEL (2019) *Algunos Aspectos Jurídicos Del Cifrado De Comunicaciones*. Derecho PUCP, n.º 83 (noviembre), 241-62
- ÁLVAREZ VALENZUELA, DANIEL (2020) *La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. Santiago: Revista Chilena de Derecho y Tecnología*. Vol. 9, N°1, págs. 1-4.
- ANÓNIMO (s/f) *Código de Hammurabi* [en línea] Edición Luarna. Disponible en < http://www.ataun.eus/BIBLIOTECAGRATUITA/Cl%C3%A1sicos%20en%20Espa%C3%B1ol/An%C3%B3nimo/C%C3%B3digo%20de%20Hammurabi.pdf> [Visto en línea 10/05/2021]

- BELTRÁN D. DANIEL (2004) *Diseño y estudio de redes de telefonía celular. Tesis profesional para obtener el título de Ingeniero Eléctrico*. Universidad Autónoma de San Luis de Potosí. Facultad de Ciencias. Disponible en línea en https://ninive.uaslp.mx/xmlui/bitstream/handle/i/1857/IEL1DER00401.pdf?sequence=3&isAllowed=y [Visto en línea 15/11/2021]
- BENUSSI, CARLOS (2020) *Obligaciones de seguridad en el tratamiento de datos personales: Escenario actual y desafíos regulatorios pendientes*. Santiago de Chile: Revista de Derecho y Tecnología vol. 9 num. 1 (2020), págs. 227 – 279.
- BIOBÍO (2020) *Entra en vigencia ley "Chao Dicom": encargados de registros tendrán 6 meses para adecuarse* [en línea] <https://www.biobiochile.cl/especial/educacion/noticias/2020/03/02/entra-en-vigencia-ley-chao-dicom-encargados-de-registros-tendran-6-meses-para-adecuarse.shtml> [Visto en línea 10/04/2020]
- BORGES, RAQUEL (2018) *La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea*. Rev. Bol. Der. no.25 Santa Cruz de la Sierra 2018
- BRAUN, ELIÉCER (1992) *Electromagnetismo, de la ciencia a la tecnología. Capítulo XVIII "Inicio de las comunicaciones inalámbricas. Marconi*". Ed. Fondo de Cultura Económica. Primera Edición, México. Disponible on-line en http://omega.ilce.edu.mx:3000/sites/ciencia/volumen 3/ciencia3/112/htm/electr.htm. [Visto en línea 11/10/2021]
- BUENO DE MATA, FEDERICO (2014) *Prueba Electrónica y Proceso 2.0,* Valencia: Tirant lo Blanch
- CABELLO GIL, LAURA M. (2017) *Datos de geolocalización como medida de investigación. Avances en el sistema jurídico procesal penal*. Tesis Doctoral. España, Facultad de Derecho de Universidad Nacional de Educación a Distancia.
- CANALES, MARÍA PAZ; LARA, JUAN CARLOS (2018) *La construcción de estándares legales para la vigilancia en América Latina Parte III: propuesta de estándares legales para la vigilancia en Chile.* Santiago de Chile: Derechos Digitales

- CAROCCA, ALEX (1998*) Garantía constitucional de la defensa procesal*. Barcelona: Ed. J.M. Bosch.
- CASARINO VITERBO, MARIO (1984) *Manual de Derecho Procesal, tomo IV,* cuarta edición. Santiago de Chile: Editorial Jurídica de Chile.
- CHAHUÁN, SABAS (2012) *Manual del Nuevo Procedimiento Civil*. Editorial Thomson Reuters. Chile
- COCIÑA, MARTINA (2012) *La verdad como finalidad del proceso penal.* Santiago de Chile: Thomson Reuters
- COLEGIO DE INGENIEROS DE CHILE (2019) *Informe pericial de Eduardo Costoya para la causa Rol 1100-2018, 4° Juzgado de Garantía de Santiago.*
- COLOMBO, JUAN. (2006) *El debido proceso constitucional.* Santiago de Chile: Tribunal Constitucional, Cuadernos del Tribunal Constitucional N°32, 2006.
- CONTRALORÍA GENERAL DE LA REPÚBLICA. 24 de noviembre de 2017. *Dictamen 041188N17. Representa el decreto N°866, de 2017, del Ministerio del Interior y Seguridad Pública.* [en línea] https://www.contraloria.cl/pdfbuscador/dictamenes/041188N17/html> [Visto en línea 18/11/2019]
- CORTE SUPREMA (2019) Oficio N° 23 – 2019. *Informe proyecto de Ley N° 2-2019. [en línea]. 12 de febrero de 2019.* Antecedente: Boletín N° 12.192-25 <https://www.pjud.cl/documents/396729/0/INFORME+PROYECTO+DE+LEY+CONVENIO+BUDAPEST.pdf/f1b87b83-ee25-4ff7-b605-925f5319577e> [Visto en línea 01/12/2019]
- DE AGUILAR GUALDA, SALUD (2019) *La prueba digital en el proceso judicial. Ámbito Civil y Penal*. [en línea] Barcelona: Bosch Editor. Disponible en https://www-digitaliapublishing-com.uchile.idm.oclc.org/visor/62844 [Visto en línea 10/10/2020]
- DE LA PEÑA, JOSÉ. *Historia de las Telecomunicaciones*. Ariel Derecho, 2003
- DÍAZ, MARIANNE (2017) *Retención de datos y registro de teléfonos móviles. [en línea] Derechos Digitales. Chile*. 9p. <https://www.derechosdigitales.org/wp-content/uploads/informe-marianne-retencion-de-datos.pdf> [Visto en línea 03/12/2029]

- DONOSO, LORENA (2020*) Primer Congreso Estudiantil de Derecho y Tecnología: Desafíos Tecnológicos en la nueva Constitución. Facultad de Derecho Universidad de Chile*. Disponible en https://www.youtube.com/watch?v=jNWzl55e0lI&t=6007s&ab_channel=uchilederecho [Visto en línea 20/11/2020]
- ELÍAS PUELLES, RICARDO (2016) *Decreto Legislativo 1182, Geolocalización y Proceso Penal*. Lima, Perú, Hiperderecho
- ENACOM (s.a.*) ¿Qué es el IMEI?* [en línea] <https://www.enacom.gob.ar/imei> [Visto en línea 10/04/2020]
- FERNÁNDEZ, JOSÉ JULIO (2016*) Los datos de trafico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente*. Revista Española de Derecho Constitucional N°108, 93-122.
- GARCÍA MATEOS, JOSÉ AURELIO (2016) *Cadena de custodia vs mismidad. Disponible en: La prueba electrónica, validez y eficacia procesal*. Colección Desafíos legales Juristas con Futuro. 131p.
- GASCÓN ABELLÁN, MARINA (2010) *Los hechos en el derecho*. Bases argumentales de la prueba. Tercera edición. Madrid: Marcial Pons
- GÓMEZ LARA, CIPRIANO (2012) *Teoría general del proceso.* Décima edición. D.F. de México: Oxford University press
- GONZÁLEZ I JIMÉNEZ, ALBERT (2014*) Las diligencias policiales y su valor probatorio.* España: Bosch Editor.
- HEGEL, FRIEDRICH (s/f) *Principios de la filosofía del derecho o derecho natural y ciencia política*. Edición Ebook Anónima.
- HERRÁN, ANA ISABEL (2003) *EL derecho a la protección de los datos personales en la sociedad de la información.* En Cuadernos Deusto de Derechos Humanos, Universidad de Deusto: Bilbao
- HORAK, RAY (2007) *Telecommunications and Data Communications Handbook*, EE. UU.: Wiley

- IEEE (1983) *Standard Definitions of Terms for Antennas, Std 145-1983, Revision of ANSI/IEEE Std 145-1973* [en línea] <https://ieeexplore.ieee.org/document/30651> [Visto en línea 15/11/2021]
- INSTITUTO CHILENO DE DERECHO Y TECNOLOGÍA (2017) *Posición del ICDT frente al Decreto Nº 866/2017, que establece un sistema general de vigilancia de la población* [en línea] 30 de agosto de 2017. <https://www.icdt.cl/orwell-en-chile/> [Visto en línea 10/10/2020]
- IVELIC MANCILLA, ALEJANDRO (2014) *Las interceptaciones de comunicaciones telefónicas en los delitos de tráfico ilícito de estupefacientes*. Revista Jurídica del Ministerio Público. N° 60, septiembre 2014
- LARA, JUAN CARLOS; PINCHEIRA, CAROLINA; VERA, FRANCISCO (2014) *La privacidad en el sistema legal chileno.* ONG Derechos Digitales. P. 70 Disponible en línea https://www.derechosdigitales.org/wp-content/uploads/pp-08.pdf [Visto en línea 11/11/2021]
- LAUDAN, LARRY (2011) *El estándar de prueba y las garantías en el proceso penal*. Buenos Aires: Hammurabi
- LÓPEZ BETANCOURT, EDUARDO (2017) *Juicios orales en materia penal.* México: Iure Editores
- MAÑAS MARÍN, CRISTINA (2018) *La localización del sospechoso mediante dispositivos de seguimiento y su aplicación en el proceso penal*. *Prueba ilícita*. Trabajo de grado de Derecho. Colegio Universitario de Estudios Financieros
- MAQUEO, MARÍA SOLANGE; MORENO, JIMENA; RECIO, MIGUEL (2017) *Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario*. Revista de Derecho vol. XXX N° 1.
- MATURANA, CRISTIAN & MONTERO, RAÚL (2010) *Derecho Procesal Penal, tomos I y II,* Santiago de Chile: Legal Publishing
- MATURANA, CRISTIAN & MONTERO, RAÚL (2017) *La necesidad de establecer un estándar de prueba en el nuevo proceso civil chileno*. Santiago de Chile: Librotecnia
- MELIÁ MIRALLES, JOAQUÍN (1991) *Fundamentos físicos de la teledetección: leyes y principios básicos;* En la teledetección en el seguimiento de los recursos naturales, Universidad de Valencia [en línea]

https://books.google.cl/books?id=t8ZLSpM20m8C&pg=PA51&redir_esc=y#v=onepage&q&f=false [Visto en línea 17/11/2021]

- MENDOZA, E.; PUERTAS, JOSÉ; MONTERO, JOSÉ (2017) *Antenas sectoriales [*en línea] <https://es.slideshare.net/ErnestoMendoza10/antenas-sectoriales> [Visto en línea 15/11/2021]
- MOLINA, OSCAR (2018) *La protección de datos personales es un derecho constitucional.* [En línea] https://www.az.cl/la-proteccion-de-los-datos-personales-es-un-derecho-constitucional/ [Visto en línea 07/01/2022]
- NARANJO E IBARROLA ABOGADOS (2019) *Aspectos Generales de la Prueba:* basado en la separata de Maturana 2015
- NATAL MARCOS, NATALIA (2020) *La cadena de custodia: algunos problemas específicos de exclusión probatoria.* Facultad de Derecho Universidad de León p. 18
- OFICINA DEL ALTO COMISIONADO DE LA ONU PARA LOS DERECHOS HUMANOS (1988) Derecho a la intimidad (Art 17) HRC Observación general N°16
- ORANGE. (s/f) *¿cómo funciona una red móvil?* [en línea] https://radio-waves.orange.com/es/como-funciona-una-red-movil/ [Visto en línea 17/03/2020]]
- OVALLE FAVELA, JOSÉ (2016) *Teoría General del Proceso*. 7ma Edición, Ciudad de México: Oxford University Press
- PÉREZ GIL, JULIO (2010) *Los datos sobre localización geográfica en la investigación penal.*
- PRIORI POSADA, GIOVANNI (2019) *El proceso y la tutela de los derechos.* Lima: Pontificia Universidad Católica del Perú, Fondo Editorial
- RAMÍREZ ZARATE, GUIMER (2014) *Implementación de seguridad domiciliaria mediante comandos AT sobre la tecnología de telefonía móvil*. Memoria para optar al grado de licenciado en electrónica y telecomunicaciones, Facultad de Tecnología Universidad Mayor de San Andrés, Bolivia. p. 14 [en línea] https://repositorio.umsa.bo/xmlui/bitstream/handle/123456789/11564/EG-1369-Ramirez%20Zarate%2C%20Guimer.pdf?sequence=1&isAllowed=y [Visto en línea 18/11/2021]

- REAL ACADEMIA DE INGENIERÍA DE ESPAÑA (s/f) *Diccionario español de ingeniería:* [en línea] http://diccionario.raing.es/es [Visto en línea 17/11/2021]
- REAL ACADEMIA ESPAÑOLA (s/f) *Diccionario de la lengua española* [en línea] https://dle.rae.es/telefon%C3%ADa. [Visto en Línea 15/11/2021]
- RODRÍGUEZ LAINZ, JOSÉ LUÍS (2011) *Estudios sobre el secreto de las comunicaciones.*
- *Perspectiva doctrinal y jurisprudencial*. [en línea] España. Wolters Kluwer España, S.A. <http://www.digitaliapublishing.com.uchile.idm.oclc.org/visorepub/49177> [Visto en línea 18/11/2020]
- RODRIGUEZ, KATITZA & ALIMONTI, VERIDIANA (2021) *A pesar del progreso, los metadatos aún tienen una protección de "segunda clase" en Latam.* EFF. Disponible en https://www.eff.org/es/deeplinks/2021/02/despite-progress-metadata-still-under-second-class-protection-latam-legal [Visto en línea 10/01/2022]
- ROLÓN, DARIO (2017) *Intercepción de metadatos de comunicaciones por teléfonos móviles. El IMSI-Catcher y su regulación en el ordenamiento procesal penal alemán*. Revista de Estudios de Justicia, N°27, págs. 61-79, Santiago.
- ROXIN, CLAUS (2000) *Derecho Procesal Penal.* Traducción 25° edición alemana. Buenos aires: Editores del Puerto
- SALAZAR, JORDI (2016) *Redes inalámbricas, České vysoké učení technické v Praze Fakulta elektrotechnická, (only electronic form). TechPedia. European Virtual Learning Platform for Electrical and Information Engineering.* http:///www.techpedia.eu. Disponible en línea en https://upcommons.upc.edu/bitstream/handle/2117/100918/LM01_R_ES.pdf [Visto en línea 11/10/2021]
- SAPIENSMAN (s/f) *Historia de la comunicación por alambres: inicios del telégrafo y el teléfono, publicación electrónica, disponible on-line*: http://www.sapiensman.com/old_wires/telegrafo_y_telefono3.htm [Visto en línea 11/10/2021]
- SCENIH (2008) *Scientific Comittee on Emerging and Newly Identified Health Risks. Light Sensivity. Adopted an 26TH Plenary on 23.09.2008.* Disponible en línea en

https://ec.europa.eu/health/ph_risk/committees/04_scenihr/docs/scenihr_o_019.pdf [Visto en línea 15/11/2021]

- SILVA BASCUÑÁN, ALEJANDRO (2006) *Tratado de Derecho Constitucional, tomo XI*. 2° Edición. Santiago de Chile: Editorial Jurídica de Chile.
- TARUFFO, MICHELE (2008) *La prueba.* Madrid: Marcial Pons
- TECHOPEDIA (s/f) *¿Qué significa red celular*? [en línea] https://www.techopedia.com/definition/24962/cellular-network [Visto en línea 17/11/2021]
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (s/f) *Términos y definiciones (traducción libre)* [en línea] < https://www.itu.int/br_tsb_terms/ [Visto en línea 17/11/2021]
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (1989) *Reglamento de telecomunicaciones internacionales [En línea]* https://www.itu.int/dms_pub/itu-t/oth/3F/01/T3F010000010001PDFS.pdf [Visto en línea 15/11/2021]
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (1993) *UTI-R V.662-2. Recomendación UIT-R V.662-2 "Términos y definiciones (1986-1990-1993).* [En línea] https://www.itu.int/dms_pubrec/itu-r/rec/v/R-REC-V.662-2-199304-S!!PDF-S.pdf [Visto en línea 15/11/2021]
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (2015) *Paris 1865: Nacimiento de la Unión. Documento publicado con ocasión del 159° aniversario de la Creación de la Unión Internacional de las Telecomunicacione*s, Publicación electrónica. Disponible on-line en https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/12.36.72.es.300.pdf [Visto en línea 20/10/2021]
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (2015*) Manual sobre la gestión nacional del espectro*. Disponible en línea en https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-21-2015-PDF-S.pdf. [Visto en línea 15/11/2021]
- UNIÓN INTERNACIONAL DE TELECOMUNICACIONES (2021) *Traducción libre del texto: "Installation intended to provide access to the telecommunication system by means of radio waves." ITU-T, K.56 (05/2021), Series K: Protection against*

interference. Protection of radio base stations against lightning discharches". Disponible en línea en https://www.itu.int/rec/T-REC-K.56-202105-I/es [Visto en línea 15/11/2021]

- VÁZQUEZ, RUBÉN. (2016) *Geolocalización y practica probatoria, condenados a encontrarse. Disponible en: La prueba electrónica, validez y eficacia procesal. Colección Desafíos legales Juristas con Futuro.*
- VIOLLIER, PABLO (2019) *¿Quién defiende tus datos? [en línea] Derechos Digitales América Latina ONG.* <https://www.derechosdigitales.org/wp-content/uploads/quien-defiende-tus-datos-2019.pdf> [Visto en línea 25/10/2019]
- VIVANCO, ÁNGELA. (2006) Curso de Derecho Constitucional: aspectos dogmáticos de la Carta Fundamental. Tomo II, 2° edición. Santiago de Chile: Ediciones Universidad Católica de Chile
- WOM (2020) *Protocolo de entrega de información a la autoridad año 2020* [en línea] <http://www.wom.cl/bases/bases/documents/Protocolo-Entrega-Informaci%C3%B3n-Autoridad.pdf> [Visto en línea 16/04/2020]

Instrumentos de Derecho Internacional[334]

- OEA (1948) Declaración Americana de los Derechos y Deberes del Hombre. Aprobada en la Novena Convención Internacional Americana, Bogotá, Colombia, 1948.

Proyectos de ley de Chile

- MOCIÓN PARLAMENTARIA (2014) Boletín N°9.384-07: Proyecto de reforma constitucional, iniciado en moción de los Honorables Senadores señores Harboe, Araya, Lagos, Larraín y Tuma, que consagra el derecho a la protección de los datos personales. Chile.
- MENSAJE PRESIDENCIAL (2017) Boletín N°11.144-07: Proyecto de ley, iniciado en mensaje de S. E. la Presidenta de la República, que regula la protección y el tratamiento

[334] El resto se encuentra en la sección de leyes chilenas, que los incorporan al ordenamiento nacional.

de los datos personales y crea la Agencia de Protección de Datos Personales [en línea] Ingresado el 11 de marzo de 2017. p. 1 <https://www.camara.cl/verDoc.aspx?prmID=11456&prmTIPO=INICIATIVA> [Visto en línea el 26/04/2020]

- PRESIDENTE DE LA REPÚBLICA (2017) Proyecto de Decreto Supremo 866 de 2017. [en línea] Disponible en: < https://www.derechosdigitales.org/wp-content/uploads/decreto-866-2017.pdf> [Visto en línea 08/02/2021]
- MENSAJE PRESIDENCIAL (2018) Boletín N°12.192-25: Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest

b. Ordenamiento Jurídico Chileno

- CHILE. Ministerio de Transporte. (1977) *Decreto Ley 1762: Crea la Subsecretaria de Telecomunicaciones dependientes del Ministerio de Transportes y organiza la Dirección Superior de las Telecomunicaciones del país.* 30 de abril de 1977
- CHILE. Ministerio de Transporte y Telecomunicaciones (1982) *Ley 18.168: Ley General de Telecomunicaciones.* Publicada el 02 de octubre de 1982
- CHILE. Ministerio de Relaciones Exteriores (1989) *Decreto 778: Promulga el Pacto Internacional de Derechos Civiles y Políticos adoptado por la Asamblea General de las Naciones Unidas por Resolución N°2.200, el 16 de diciembre de 1966 y suscrito por Chile en esa misma fecha*. Publicada 29 de abril de 1989.
- CHILE. Ministerio de Relaciones Exteriores (1991) *Decreto 873: Aprueba la Convención Americana sobre Derechos Humanos, denominada "Pacto de San José de Costa Rica*". Publicada el 5 de enero de 1991
- CHILE. Ministerio Secretaría General de la Presidencia (1999) *Ley N° 19.628: sobre protección de la vida privada.* 28 de agosto de 1999
- CHILE. Ministerio de justicia (2000) *Ley 19.696: Código Procesal Penal*. 12 de octubre de 2000

- CHILE. Ministerio de Economía, fomento y reconstrucción (2002*) Ley N°19.799: Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma*. Publicada el 12 de abril de 2002.
- CHILE. Ministerio de Transporte y Telecomunicaciones (2004) *Decreto 510: establece el contenido mínimo y otros elementos de la cuenta única telefónica, y modifica reglamento del servicio público telefónico, y reglamento para el sistema multiportador discado y contratado del servicio telefónico de larga distancia nacional e internacional*
- CHILE. Ministerio Secretaría General de la Presidencia (2005) *Decreto 100: Fija el texto refundido coordinado y sistematizado de la Constitución Política de la República de Chile*, 22 de septiembre de 2005.
- CHILE, Ministerio de transportes y telecomunicaciones (2005) *Decreto 142/2005: Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de telecomunicación*. Publicado el 22 de septiembre de 2005.
- CHILE. Ministerio de transportes y telecomunicaciones; subsecretaría de las telecomunicaciones (2006*) Decreto 127. Aprueba plan general de uso del espectro radioeléctrico*. Publicado el 18 de abril de 2006.
- CHILE. Ministerio de Transporte y Telecomunicaciones (2012) *Decreto194: aprueba reglamento sobre tramitación y resolución de reclamos de servicios de telecomunicaciones.* 16 de febrero de 2013
- CHILE. Ministerio de Transporte y Telecomunicaciones (2013) *Decreto 22: Reglamenta la forma y condiciones para el emplazamiento de antenas y sistemas radiantes y sus torres soportantes respecto de servicios de telecomunicaciones distintos a los referidos en la letra b) del artículo 3º de la ley general de telecomunicaciones*. Fecha 28 mayo 2013
- CHILE Ministerio de Transportes y Telecomunicaciones, Subsecretaria de Telecomunicaciones. (2014) *Decreto 18: Aprueba Reglamento de Servicios de Telecomunicaciones que indica*. Publicado el 13 de febrero de 2014
- CHILE Ministerio de Relaciones Exteriores (2017) *Promulga el Convenio sobre la Ciberdelincuencia*. Publicado el 28 de agosto de 2017
- CHILE. Ministerio Secretaría General de la Presidencia (2018) *Ley 21.096: Consagra el derecho a la protección de los datos personales*. Publicada el 16 de junio de 2018

- CHILE. Ministerio del Interior y Seguridad Pública (2019) *Ley 21.170: Modifica el tratamiento de las penas de los delitos de robo y receptación de vehículos motorizados o de los bienes que se encuentran al interior de éstos, y establece las medidas que indica*. Publicada el 26 de Julio de 2019.
- CHILE. Ministerio de Educación (2020) *Ley 21.214: Modifica la Ley N°19.628, sobre protección de la vida privada, con el objeto de prohibir que se informe sobre las deudas contraídas para financiar la educación en cualquiera de sus niveles*, febrero de 2020.

c. Normativa de la Unión Europea

- UNIÓN EUROPEA. Parlamento Europeo y Consejo (2002) *Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas -Directiva sobre la privacidad y las comunicaciones electrónicas-*, DOUE, núm. 201, de 31 de julio de 2002.
- UNIÓN EUROPEA. Parlamento Europeo y Consejo (2006) *Directiva 2006/24/CE, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE,* DOUE, núm. 105, de 13 de abril de 2006.
- UNIÓN EUROPEA. Parlamento Europeo y Consejo (2016) *Reglamento (UE) 2016/679 de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (Reglamento general de protección de datos)

d. Ordenamiento Jurídico Español

- ESPAÑA. Ministerio de Gracia y Justicia (1882) *Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.* (17/09/1882)

- ESPAÑA. Constitución Española (1978) [en línea] https://app.congreso.es/consti/constitucion/indice/index.htm> [Visto en línea 18/11/2019]

- ESPAÑA. Jefatura de Estado (2014) *Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.*
- ESPAÑA. Jefatura de Estado (2018) *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. 5 de diciembre de 2018.
- ESPAÑA. Ministerio Fiscal (2019) *Circular 4/2019, de 6 de marzo, de la Fiscal General del Estado, sobre utilización de dispositivos técnicos de captación de la imagen, de seguimiento y de localización. Boletín Oficial del Estado N°70*, de 22 de marzo de 2019, pp. 30138-30158

e. Ordenamiento Jurídico Peruano

- PERÚ. Ministerio de Justicia y Derechos Humanos (2015) *Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.* Publicado el 27 de julio de 2015

d. Jurisprudencia chilena

- CORTE DE APELACIONES DE CONCEPCIÓN (2019) *Sentencia de 17 de septiembre de 2019, ROL 731-2019*. Citado en página 58
- CORTE SUPREMA (2005) *Rol N°740-2005.* Citada en página 76
- CORTE SUPREMA. (2005) *11.5.2005. Revista Procesal Pena*l *N° 35*. Págs. 55 y Sgtes. Mayo 2005. Citado en p. 33

- TRIBUNAL CONSTITUCIONAL (2011) *Roles acumulados N°1732-10 y 1800-10 De 21 de junio de 2011, sobre publicación de las remuneraciones de altos ejecutivos de Televisión Nacional de Chile.* Citada en página 95
- TRIBUNAL CONSTITUCIONAL (2011) *Sentencia rol 2153-2011, 11 de septiembre de 2012, sobre Acceso a la Información Pública y correos electrónicos*. Citado en página 76
- 4° JUZGADO DE GARANTÍA (2018). *Causa ROL O-1100-2108. Expediente Electrónico.* Citado en página 27, nota al pie a propósito del informe del Colegio de Ingenieros.

f. Jurisprudencia Española

- TRIBUNAL SUPREMO DE ESPAÑA, Sala de lo Penal (2019) *Sentencia número 100/2019*. Citado en página 103