

DERECHO FUNDAMENTAL AL SECRETO E INVIOABILIDAD DE LAS COMUNICACIONES: ANÁLISIS COMPARADO DE SU SENTIDO Y CONTENIDO

FUNDAMENTAL RIGHT TO THE SECRECY AND INVIOABILITY OF COMMUNICATIONS: A COMPARATIVE ANALYSIS OF ITS MEANING AND CONTENT

Raffo Velásquez Meléndez*
RVM Abogados

The author conducts a thorough analysis of the fundamental right to the secrecy and inviolability of communications from a jurisprudential, doctrinal, and legislative perspective, taking into account the challenges posed by technological advancements. The author asserts that this constitutional right ensures the protection of communications against arbitrary interferences, particularly in a context where the widespread use of the internet and mobile devices has heightened the risk of privacy infringements. Furthermore, the author contends that any restriction on this right is only permissible in exceptional circumstances, subject to prior judicial authorization and strict adherence to the principle of legality.

In substantiating the study, the author draws upon constitutional provisions, international human rights instruments, and comparative law, all of which recognize this right as a cornerstone of the rule of law. Moreover, it is underscored that any limitation on this fundamental guarantee must be expressly prescribed by law, adhere to the principles of necessity and proportionality, and be subject to rigorous judicial scrutiny.

KEYWORDS: *Right to privacy; right to respect for private life; elements of the communication process; confidentiality of communications; reasonable expectation of privacy.*

El autor realiza un análisis exhaustivo del derecho fundamental al secreto y la inviolabilidad de las comunicaciones desde una perspectiva jurisprudencial, doctrinal y legislativa, atendiendo a los desafíos que plantea el desarrollo tecnológico. Asimismo, considera que este derecho constitucional garantiza la protección de las comunicaciones frente a injerencias arbitrarias, especialmente en un contexto donde el uso de internet y dispositivos móviles ha incrementado el riesgo de vulneraciones a la privacidad; y que su restricción solo es admisible en supuestos excepcionales, bajo autorización judicial previa y con estricta observancia del principio de legalidad.

Para fundamentar su estudio, el autor se apoya en las disposiciones constitucionales, los instrumentos internacionales de derechos humanos y el Derecho Comparado, todos ellos coincidentes en reconocer este derecho como un pilar esencial del Estado de Derecho. Asimismo, se destaca que cualquier restricción a esta garantía debe estar expresamente prevista en la ley, cumplir con los principios de necesidad y proporcionalidad, y estar sujeta a un control jurisdiccional efectivo.

PALABRAS CLAVE: *Derecho a la intimidad; derecho a la privacidad; elementos del proceso de comunicación; secreto de las comunicaciones; expectativa razonable de privacidad.*

* Abogado. Magíster por la Università degli studi di Palermo y Universidad Castilla La Mancha. Socio de RVM Abogados (Lima, Perú). Código ORCID 0000-0002-1208-5959. Contacto: rvelasquez@rvmlegal.com

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 19 de abril de 2025, y aceptado por el mismo el 13 de octubre de 2025.

I. INTRODUCCIÓN

Las nuevas tecnologías plantean desafíos inéditos a la protección de la vida privada al generar riesgos sustantivos que trascienden los paradigmas tradicionales. La magnitud de los cambios es tal que los mecanismos previstos originariamente por el constituyente —como la telefonía fija, el telegrama o las cartas— han quedado obsoletos en términos prácticos, pese a regularse aún bajo el principio de la inviolabilidad de las comunicaciones.

Esta disrupción tecnológica exige una delimitación dogmática del contenido esencial de este derecho, a fin de determinar sus posibilidades de desarrollo y adaptación. Precisamente, este será nuestro propósito en el presente artículo.

Para tal efecto, indagaremos en la noción jurídica de vida privada, a fin de delimitar conceptualmente los ámbitos de la intimidad y privacidad, así como su relación con el ‘secreto de las comunicaciones’ como manifestación específica del derecho a la vida privada.

El asunto tiene especial trascendencia en el Perú, donde casos paradigmáticos han evidenciado la tensión entre el derecho de prueba en el ámbito penal y la garantía del secreto de las comunicaciones. Así lo demuestran, en primer lugar, los llamados ‘petroaudios’, cuya difusión masiva de interceptaciones telefónicas ilegales generó un escándalo mediático y político, pero supuso una grave violación del artículo 2.10 de la Constitución Política del Perú (en adelante, la Constitución), lo que motivó su exclusión como medio probatorio. En el segundo caso, conocido como los ‘cuellos blanco del puerto’, si bien la interceptación telefónica se inició con una autorización judicial para la investigación de una presunta banda de narco-trafficantes, extorsionadores y sicarios, las interceptaciones telefónicas trascendieron el propósito de las autorizaciones judiciales originales, lo que motivó también a que se discuta sobre la validez de esas pruebas.

La primacía de la cultura del espectáculo ha desplazado el debate sobre derechos fundamentales hacia el escándalo mediático. Debemos evitar ese reduccionismo, prescindir de prejuicios y valoraciones subjetivas, centrarnos en un análisis constitucional objetivo. Para asegurarnos de ello, recurriremos a fuentes normativas y jurisprudenciales de los tribunales internacionales —así como a ordenamientos jurídicos comparados que han influido en nuestro ordenamiento jurídico— no solo para contrastar las soluciones jurídicas ya adoptadas por el Tribunal Constitucional (en adelante, TC), sino principalmente para integrar vacíos e insuficiencias legales y doctrinales, así como corregir los errores de comprensión de los que adolece nuestro sistema jurídico.

Veremos que definir los contenidos y alcances normativos de los derechos a la vida privada y al secreto de las comunicaciones no se agota en el plano dogmático, sino que exige necesariamente un análisis práctico y casuístico, pues es un asunto que se enfoca más en las situaciones reales de la vida.

II. DIMENSIONES DE LA VIDA PRIVADA

La versión moderna del derecho a la vida privada evidencia que su ámbito de protección no se circunscribe exclusivamente a un contenido de índole íntimo, sino que se extiende a toda situación en la que el titular manifieste ‘expectativas razonables de privacidad’, independientemente de la naturaleza material del acto o información involucrada.

La concepción clásica del derecho a la intimidad, limitada a su dimensión material, presentaba un problema práctico al vincular su protección únicamente a asuntos que el titular del derecho decide mantener en reserva, esto es, asuntos de naturaleza sensible o personalísima. La evolución jurisprudencial ha superado este enfoque, reconociendo una dimensión formal que protege la voluntad de reserva, con independencia de si su contenido es materialmente íntimo o no¹. Al respecto, en el fundamento octavo de la sentencia 144/1999 del TC español, ha señalado que el derecho a la intimidad:

¹ La experiencia y conveniencia del paso de la dimensión material a la formal del derecho a la intimidad son explicadas por López Bofill de la siguiente manera:

El camino hacia una determinación sustantiva del derecho a la intimidad estaba plagado de vaguedades, se señalaban ámbitos puntuales y fragmentarios de protección sin atreverse a perfilar nitidamente su objeto, siempre manejando intuiciones en torno a una zona —brumosa— inmediatamente circundante al individuo, en cuyo seno éste desarrolla relaciones familiares, de afecto [...] espacio de retiro en el que resaltan aspectos concernientes a la corporalidad, a la sexualidad [...] ese intento de aprehender [...] el contenido sustancial del derecho a la intimidad se encontraba atenazado por circularidad en la definición [...] [El TC] apela a un concepto tendencialmente formal del derecho a la intimidad personal y familiar cuyo ámbito viene determinado por el propio sujeto titular del derecho. Se abjura de todo intento de aproximación sustancial al contenido de la intimidad, la caracterización de ese «meta-físico» espacio en el que el individuo se desarrolla queda completamente desgajado del razonamiento y se pasa a ensalzar puramente la versión subjetiva de la intimidad como autodeterminación informativa. Es cada titular quien decide qué es lo que puede ser comunicado a otros. (2000, pp. 1888-1889)

[...] no garantiza sin más la “intimidad”, sino el derecho a poseerla, a tener vida privada disponiendo de un poder de control sobre la publicidad de la información relativa a nuestra persona y familia, sea cual sea el contenido de aquello que se desea mantener al abrigo del conocimiento público.

Propuesta que el TC español mantiene hasta ahora en diversos pronunciamientos (Sentencia 127/2003, fundamento 7; Sentencia 89/2006, fundamento 5), indicando en su fundamento jurídico segundo del caso Sentencia 173/2011, en particular, que se garantiza:

[...] un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio.

El TC peruano también reconoce el contenido formal del derecho a la intimidad en el fundamento 22 del expediente 3485-2012-AA, denominado caso ‘Carlos Mamani’, que de manera textual establece que:

[...] los derechos a la intimidad y a la vida privada [...] no solo pueden ser vistos hoy desde una óptica material en el sentido de que queden protegidos bajo su ámbito normativo aquellos datos, actividades o conductas que materialmente puedan ser calificadas de íntimas o privadas, sino también desde una óptica subjetiva, en la que lo reservado será aquello que el propio sujeto decida, brindando tutela no solo a la faz negativa del derecho (en el sentido del derecho a no ser invadido en ciertos ámbitos), sino a una faz más activa o positiva (en el sentido del derecho a controlar el flujo de información que circule respecto a nosotros).

El TC peruano aplicó este criterio para cuestionar un proceso disciplinario iniciado en contra de fiscales por mantener relaciones extramatrimoniales, lo que se pretendía probar mediante un video obtenido de manera ilegal que grababa el ingreso forzoso de unas personas a un cuarto de hotel con el propósito de captar un encuentro sexual en el que estaban involucrados tales funcionarios. De un lado, el TC consideró que dicha conducta lesionaba el derecho a la intimidad, por invadir un espacio en donde existe una ‘expectativa razonable de privacidad’. A su vez, ante el intento de usar ese video para acreditar una falta al deber de integridad exigido por el interés público, el TC, en el denominado caso ‘Carlos Mamani’, señaló que el ca-

rácter sensible de los encuentros sexuales carecía de relevancia para los intereses públicos y que, por el contrario, el uso de ese video exponía aspectos personalísimos que atentaban la intimidad (Expediente 3485-2012-AA, fundamento 34).

Lo anterior evidencia que el derecho a la vida privada establece distintos límites, según el momento del agravio. Por ejemplo, con anterioridad a cualquier intromisión, los terceros tienen como límite ineludible la exigencia de respetar aquellos espacios en los que existe ‘expectativa razonable de privacidad’, con independencia del contenido íntimo o no de la información existente en tales espacios. Por tanto, les está vedado acceder a domicilios, oficinas, habitaciones de hotel, cabinas telefónicas o, en general, a cualquier ámbito en el que es razonable pensar que se busca excluir el conocimiento de otros.

El hecho de que terceros irrumpen la valla de lo reservado conlleva la activación de otros límites tanto formales como materiales. En tal supuesto, no podrán usar, difundir o mantener la información obtenida, ya sea por tratarse de datos intrínsecamente íntimos o porque el titular haya manifestado que quiere mantener su carácter reservado, aunque su contenido no revista naturaleza íntima.

En otras palabras, la dimensión formal del derecho a la intimidad opera como una esfera de protección preventiva del derecho a la intimidad, aplicable tanto en los momentos iniciales –antes de que ocurra una intromisión en espacios reservados– y, en algunas ocasiones, luego de dichas intromisiones. Por su parte, la dimensión material de este derecho adquiere relevancia una vez consumada la intromisión, cuando se discute el almacenamiento o la eventual difusión de aquellos datos que, por su naturaleza intrínsecamente íntima o personalísima –o por expresa voluntad del titular–, merecen especial protección jurídica.

III. MOMENTOS EN LOS QUE ACTÚAN LAS DIMENSIONES DE LA VIDA PRIVADA

Inicialmente, el derecho a la intimidad despliega una protección de carácter formal, que se traduce en la prohibición absoluta a cualquier tercero de acceder a espacios reservados, con independencia de la naturaleza íntima o no de su contenido. En esta fase, la mera intromisión injustificada en dichos ámbitos constituye una agresión a la intimidad.

Sin embargo, una vez vulnerada dicha barrera protectora inicial, este derecho mutará, en su régimen de tutela, pues su objetivo ya no será prevenir la intromisión, sino restablecer la reserva quebrantada. Esta nueva fase, impone obligaciones concre-

tas: la restitución o eliminación de la información ilícitamente obtenida, o la prohibición absoluta de su difusión. Tales medidas operan tanto cuando el titular insiste en que se mantenga el carácter reservado de la información como cuando revisten, *per se*, caracteres intrínsecamente íntimos.

Por ejemplo, si un periodista emplea un dron para tomar fotos de la mascota de un personaje público dentro de su casa, el afectado podrá exigir la destrucción de las fotos —aun cuando el contenido no revista carácter íntimo— por invadir un espacio reservado. No obstante, si las fotos hubieran registrado a la persona afectada en estado de desnudez o en una discusión con un familiar, se podrá agregar el argumento material y, con ello, la obligación de destruir las fotografías por constituir datos intrínsecamente íntimos.

Algunas veces puede justificarse el acceso y difusión de los datos alegando que su contenido atañe al interés público (como la revelación de hechos noticiosos, delitos u otros valores constitucionalmente superiores). En tales casos, la tutela formal basada en la ‘expectativa razonable de privacidad’ deberá ponderarse con dichos intereses contrapuestos. Este análisis determinará si la divulgación esta constitucionalmente amparada por su contribución al interés público² o si, por el contrario, prima el derecho a la intimidad por carecer de la información de interés público.

Por tanto, cuando se pretende difundir información protegida por una ‘expectativa razonable de privacidad’, resulta imperativo realizar un juicio de ponderación para determinar la existencia de un interés público en ello. Si no existe, prevalecerá la protección formal del derecho a la intimidad, proscribiéndose su difusión (sin importar su contenido íntimo o no). Sin embargo, si se determina la existencia de un interés público en los datos obtenidos, se podrá difundir solo aquellos aspectos relevantes a dicho interés. Aquí, adquiere plena vigencia la dimensión material del derecho, que exige la exclusión de todo dato intrínsecamente íntimo, garantizando que la afectación a la privacidad no exceda lo indispensable para satisfacer el fin público legítimo perseguido.

Por ejemplo, si un candidato a la presidencia del país es captado huyendo del departamento en donde se originó un incendio, dicha circunstancia —por su indudable relevancia para la evaluación de su idoneidad y conducta pública— constituye información de interés público que justifica plenamente su difusión. Sin embargo, si en el mismo contexto algún periodista obtuviera fotografías de actos carnales en dicho departamento que acreditaran que el candidato tenía una relación extramatrimonial, dicha información íntima exigiría un escrutinio riguroso para definir si se puede difundir o no. Lo razonable sería concluir que no se pueden difundir esos datos explícitos, pero sí dar noticia de su existencia.

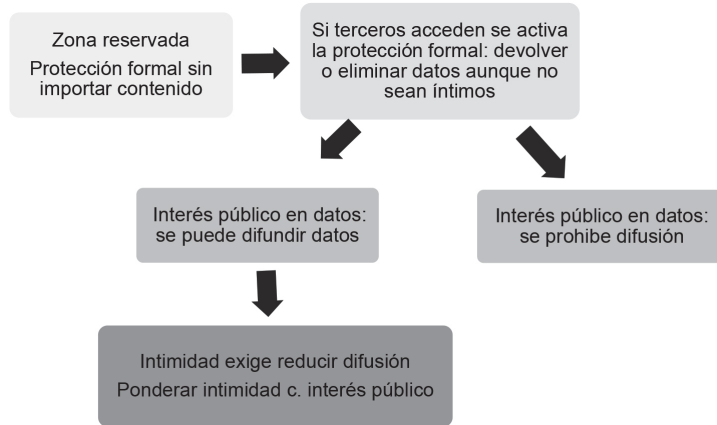
Incluso ante la existencia de interés público en la información, la garantía material del derecho a la intimidad conserva su carácter infranqueable. Este núcleo duro infranqueable permite informar sobre conductas relevantes para la vida pública, pero prohíbe compartir o difundir aquellos aspectos que atañen actos personalísimos de la privacidad. En el ejemplo propuesto, será de interés público informar sobre la relación extramatrimonial del candidato, pero no lo será difundir el acto mismo de infidelidad. En estas situaciones opera la dimensión material de la intimidad.

En el conocido caso de las ‘prostivedettes’ (Expediente 6712-2005-HC, fundamentos 56-60), un programa televisivo (Magaly Medina) denunció que personajes públicos ejercían la prostitución clandestina, difundiendo imágenes explícitas de actos sexuales. La conductora fue condenada penalmente por agraviar la intimidad de los personajes involucrados. El *habeas corpus* de la conductora llegó hasta el TC, el cual consideró que informar sobre las actividades ilícitas era un hecho noticioso, pero determinó que la exhibición de registros íntimos constituyó una vulneración al núcleo esencial del derecho a la intimidad, pues solo cabía informar sobre la existencia de los hechos.

Los momentos en el que las dimensiones formales y materiales del derecho a la intimidad entran a tallar pueden graficarse de la siguiente manera:

² Por ejemplo, en el caso del hijo extramatrimonial del expresidente argentino Carlos Menem, la Corte Interamericana de Derechos Humanos señaló que debió prevalecer el interés público sobre el dato privado porque el hecho se vinculaba con la disposición del erario y con favores laborales a la familia materna de ese hijo desconocido por la población (Sentencia del 29 de noviembre de 2011, par. 67-75). Mientras que en el caso de la princesa alemana von Hannover, el Tribunal Europeo de Derechos Humanos advirtió que no existía ningún interés público en informar sobre los paseos en bicicleta, en la playa o vacaciones de la agraviada, de modo que debía prevalecer su ‘expectativa razonable de privacidad’ (Sentencia del 24 de junio de 2004, par. 65-66, 76-77). Lo propio pasó con la difusión de las interceptaciones telefónicas del ex primer ministro italiano Silvio Berlusconi, pues el Tribunal Europeo de Derechos Humanos advirtió que eran conversaciones que no se relacionaban con el interés público, con los delitos que se le imputaban (Craxi, párrafo 66).

Gráfico 1: Dimensión formal y material del derecho a la intimidad



Fuente: Elaboración propia

IV. VÍNCULO DE LA DIMENSIÓN FORMAL CON EL SECRETO DE LAS COMUNICACIONES

En ese hilar de ideas, resulta imperativo cambiar la postura que tomamos hace quince años sobre el secreto de las comunicaciones, pues este derecho sí tiene basamento en el derecho a la intimidad. Aunque un sector de la doctrina insiste en la autonomía de ambos derechos, postulando que el primero (secreto de las comunicaciones) opera como una garantía formal que protege el proceso comunicativo en sí mismo —asegurando su reserva con independencia de su carácter íntimo o no del contenido—, mientras que el segundo (derecho a la intimidad) constituiría una tutela material dirigida específicamente a resguardar aquellos contenidos que, por su naturaleza intrínsecamente privada o personalísima, merecen especial protección jurídica.

Esta distinción doctrinal resulta conceptualmente inexacta, pues el derecho a la intimidad posee primordialmente una dimensión formal y, solo de manera excepcional, una dimensión material. El primero protege de modo absoluto los espacios objetivamente reservados, con prescindencia del valor íntimo o no de su contenido; en tanto el segundo, se activa exclusivamente cuando, existiendo un interés público en la difusión de cierta información, debe ponderarse la protección de aquellos contenidos materialmente íntimos. Esta estructura ubica al derecho al secreto de las comunicaciones como una manifestación específica

de aquella tutela formal que asegura el derecho a la intimidad³.

En ese sentido, se puede decir que los derechos al secreto y a la intimidad aspiran a proteger las mismas situaciones: espacios reservados en donde sus titulares tienen ‘expectativas razonables de secreto’. En ese sentido, el TC peruano, en el caso denominado ‘Carlos Mamani’, precisa que:

[Intimidad y privacidad] fundamentan otra serie de derechos que buscan justamente proteger ciertos espacios donde la persona pueda actuar con esa expectativa legítima de privacidad que es inherente al espacio donde su actividad se desarrolla. Así, diversos derechos reconocidos en el texto constitucional, como lo son: el derecho a la inviolabilidad del domicilio (artículo 2 inciso 9), el derecho al secreto y inviolabilidad de las comunicaciones privadas (artículo 2 inciso 10), el derecho al secreto profesional (artículo 2 inciso 18), el derecho al secreto bancario o el derecho a la reserva tributaria (artículo 2 inciso 5), permiten construir ese espacio donde la persona debe ser, en principio, invulnerable. Y aunque estos derechos tienen una naturaleza formal, en el sentido de que protegen todo lo que se desarrolla bajo esos espacios, al margen de que contengan datos sobre lo íntimo o lo privado. (Expediente 3485-2012-AA, fundamento 21)

Cuando se trata del derecho al secreto de las comunicaciones, el uso de canales cerrados de co-

³ En ese sentido, señala Rodríguez Lainz que:

[...] la interceptación de cualquier comunicación telefónica o mensaje SMS y el acceso a su contenido supondrá una vulneración del [secreto de las comunicaciones], sin necesidad de adentrarnos a cuál fuere el contenido de ésta y su mayor o menor trascendencia [...] [El TC] afirma que la noción misma del carácter formal de tal derecho responde a la idea de que «[...] se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado». (2011, p. 3)

municación permite entender que su titular ha decidido mantener en reserva el proceso comunicativo, con independencia del contenido transmitido; mientras que el derecho a la intimidad surge cuando la decisión de mantener cierta información en espacios cerrados, da a entender que su titular ha decidido mantenerla en reserva frente al conocimiento de terceros. Que el primero garantice la reserva de un proceso comunicativo y el segundo proteja los datos que el titular decide mantener en reserva, evidencia que ambos constituyen expresiones particulares de una aspiración común: la expectativa de reservar determinados ámbitos frente a la intromisión de terceros. En esta línea, se podría decir, incluso, que el derecho al secreto forma parte del contenido negativo del derecho de intimidad, esto es, de aquella dimensión que protege la esfera personal frente a perturbaciones de terceros.

Ambos aspiran a lo mismo —la protección de la esfera reservada frente a intromisiones ajenas—, diferenciándose únicamente en el régimen jurídico que le es aplicable a cada uno. El derecho al secreto goza de un nivel reforzado de protección en comparación con los espacios tutelados por la intimidad, lo que se explica por la particular vulnerabilidad que presenta el proceso comunicativo, al desarrollarse a través de canales cerrados administrados o facilitados por terceros. Esa situación genera un riesgo objetivo y permanente de interceptación o perturbación de aquello que los comunicantes han decidido mantener en secreto y que, por la propia naturaleza del medio utilizado, escapa a su control directo, exigiendo, por tanto, una salvaguarda jurídica más intensa que compense esta exposición estructural cuya protección escapa al control de los comunicantes.

Por lo demás, no sería la primera vez que otros espacios protegidos por la intimidad ameritan una protección mayor a la que ordinariamente se otorga a este derecho fundamental. Piénsese, por ejemplo, en el artículo 2.18 de la Constitución peruana, que otorga protección especial al derecho a mantener reserva o el secreto profesional en las relaciones médico-paciente, abogado-cliente e incluso entre el periodista y la persona que actúa como fuente de la información que recibe (Expediente 0134-2003-HD, fundamentos 2-3; Expediente 7811-2015-AA, fundamentos 4-8).

El desarrollo y análisis más detallado del derecho al secreto e involucabilidad de las comunicaciones —en sus contenidos, alcances y aplicación práctica— demuestra que este regula aspectos inherentes al derecho a la intimidad, pero bajo un régimen jurídico especial. Esta diferencia sustancial en sus

regímenes de protección exige identificar con precisión los supuestos que activan cada derecho, pudiendo considerarse autónomos únicamente para efectos de su implementación concreta.

V. ESTRUCTURA DEL DERECHO AL SECRETO DE LAS COMUNICACIONES

Para mayor facilidad, emplearemos la denominación ‘derecho al secreto’ para referirnos a los espacios reservados como objeto de protección, y la expresión ‘derecho a la involucabilidad’ para aludir al régimen de garantías que aseguran dicha reserva frente a intromisiones indebidas.

El derecho al secreto tutela los procesos comunicativos facilitados por terceros, estableciendo: (i) una ‘protección formal’ que se activa independientemente del carácter íntimo del contenido transmitido; y (ii) una protección que alcance a ‘todo el proceso de comunicación y sus elementos’, pues si se exhibe alguno de ellos (comunicantes, canales, fecha, hora, etc.) revelaría la existencia misma de ese proceso, cuya reserva constituye el núcleo esencial de esta garantía. Evaluemos con mayor detalle el objeto de este derecho y las consecuencias que genera.

A. Protección formal del proceso de comunicación

El formante jurisprudencial y doctrinal coinciden en que el derecho al secreto protege al proceso de comunicación en sí mismo, con independencia del contenido transmitido. En la comunicación presencial, los sujetos determinan directamente las condiciones de reserva o no de sus conversaciones, mientras que en la comunicación mediada —al depender de canales ajenos a su control— surge la necesidad de garantizar jurídicamente la confidencialidad del proceso completo, salvaguardando así la legítima ‘expectativa de privacidad’ frente a los riesgos inherentes al uso de vías de comunicación externas.

Por lo tanto, el derecho al secreto protege los procesos de comunicación, con independencia de su contenido. Su interés es que ese proceso se mantenga en una esfera reservada, por lo que impide acceder a cualquiera de los elementos que puedan dar cuenta de su existencia. En ese sentido, desde sus inicios, el TC peruano, en el caso Rodolfo Rospigliosi, ha precisado que:

[...] el concepto de “secreto” e “involucabilidad” de las comunicaciones y documentos privados [...] comprende la comunicación misma, sea cual fuere su contenido y pertenezca o no el objeto de la comunicación al ámbito de lo

personal, lo íntimo o lo reservado⁴. (Expediente 2863-2002-AA, fundamento 3)

Debido a esta indiferencia respecto al contenido de lo comunicado, nuestra Corte Suprema sigue los criterios del TC español, tribunal que en la Sentencia 114/1984, fundamento 7 y Sentencia 34/1996, fundamento 4, ha precisado que en este derecho la noción de secreto tiene un “carácter «formal», en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado”. Este carácter formal, agrega nuestra Corte, se debe a que su objeto es la confidencialidad del proceso de comunicación y de lo comunicado, con independencia de su contenido transmitido⁵.

La jurisprudencia del Tribunal Europeo de Derechos Humanos (en adelante, TEDH), española y de nuestra Corte Suprema, coinciden en reconocer que el derecho al secreto protege integralmente el proceso comunicativo—incluyendo tanto el contenido de lo comunicado como todos sus elementos accesorios—, mientras que el derecho a la intimidad protege autónomamente aquellos espacios, datos o situaciones que el titular decide libremente mantener en reserva, con independencia de que revistan o no carácter sensible, configurando así esferas de protección diferenciadas, pero complementarias en el ordenamiento jurídico.

El reconocimiento de una posición jurídica de secreto constituye una garantía esencial para preservar espacios de libertad que merecen especial protección. Piénsese en el derecho al secreto del voto o la reserva de las convicciones políticas, filosóficas y religiosas, donde el secreto busca otorgar libertad, espontaneidad e independencia a las decisiones, liberándolas de condicionamientos externos, prejuicios sociales o escrutinios de terceros que podrían atar o inclinar las decisiones

sobre aspectos de la vida que deben permanecer absolutamente libres. En esa línea, la Corte Constitucional de Colombia, en la Sentencia C-626/96 de 1996, ha señalado que el derecho al secreto debe ser entendido como “[...] la libertad de los sujetos que participan en la comunicación, frente a las arbitrarias interferencias [...]” y que

El libre ejercicio del derecho a comunicarse se afecta, hasta el extremo de hacerlo inútil, cuando el contenido de la comunicación carece de la necesaria espontaneidad, por el temor a la injerencia extraña o a la exposición pública del mensaje o del intercambio de expresiones [...].

Esta libertad solo puede ser plena si se asegura la reserva integral del proceso de comunicación—con independencia de su contenido transmitido—, permitiendo así a los participantes interactuar con absoluta espontaneidad y confianza, libres de condicionamientos o temores derivados del posible conocimiento externo de la existencia misma del proceso comunicativo. Esta protección formal se extiende, necesariamente, sobre todos los elementos constitutivos del proceso de comunicación para asegurar que se mantenga el secreto de su existencia⁶.

En ese sentido, la titularidad del derecho corresponde a todos los participantes del proceso comunicativo, independientemente de que no manifiesten su voluntad expresamente, bastando su mero acceso al canal reservado. A partir de la jurisprudencia del TC Federal alemán (en adelante, TCF), Guzy reseña que no se trata de la clásica privacidad de un sujeto que excluye a otros, sino de una ‘privacidad comunicativa’ que supone la participación de varios en un espacio reservado (2018, pp. 14-16). Por ejemplo, el matrimonio o la familia requieren de la participación de varios sujetos en espacios privados, donde múltiples personas comparten esferas privadas para el desarrollo conjunto

⁴ Una década después, el TC reiteró que se protege la comunicación con independencia de su contenido. Un empleador accedió al sistema de mensajería que facilitó a un trabajador para recabar información que luego usaría para despedirlo. El TC ordenó la reposición del trabajador al considerar que hubo una intervención ilegítima al secreto de las comunicaciones. Si bien la sentencia no tuvo un criterio uniforme, los votos de los magistrados Mesía Ramírez, Calle Hayen y Eto Cruz coincidieron en que aquel **derecho protege la comunicación con independencia de su carácter íntimo o no**. Véase los fundamentos 4, 3 y 8, respectivamente, de los votos del caso Roberto Nieves, Expediente 0114-2011-AA.

⁵ Véase el caso Alberto Fujimori, Sentencia del 7 de abril de 2009, de la Sala Penal Especial de la Corte Suprema, Expediente 19-2001, fundamento 77. Y, a su vez, el caso Ricardo Beaumont y otros, Resolución 5 que contiene el auto de apelación del 29 de septiembre de 2015, de la Sala Penal Especial de la Corte Suprema, Expediente 04-2015 “3”, fundamento 6.

⁶ Téngase en cuenta que, en esa protección formal subyace la protección de la vida privada y, con ello, de la libertad. Pace (1985: 233-234) y CaretTi (1989: 201) advierten que la “libertad” y el “secreto” son las potestades protegidas constitucionalmente por el derecho al secreto de las comunicaciones. Esto porque el derecho asegura la posibilidad de hacer llegar libremente a un destinatario ciertas formas de expresión (aspecto de la «libertad»), sin que terceros puedan conocer el contenido del mensaje (aspecto del «secreto»). A pesar de estar estrechamente vinculados y de la unidad de la situación constitucional protegida, esa libertad y secreto pueden regularse en forma diferenciada porque su afectación también es distinta. Pueden darse violaciones de la libertad, sin afectar el secreto (pe., la no entrega o bloqueo de correspondencia), o agravios al secreto que no atenten contra la libertad (pe., las escuchas telefónicas).

de su personalidad. Así, la privacidad del secreto de las comunicaciones no se caracteriza por la ausencia de otras personas, sino por su carácter reservado del acto comunicativo, el cual presupone la autodeterminación sobre el acceso a esa esfera reservada y la consecuente protección de todos los intervinientes legitimados.

B. Protección de los elementos del proceso de comunicación

El sistema estadounidense inicialmente no prohibía la intervención de las comunicaciones, al considerar que esta no constituía una invasión física de la propiedad o domicilio y, por tanto, no afectaba la privacidad. Sin embargo, en el *leading case* de 1967 (*Katz c. United States*), la Corte Suprema estableció que se debía proscribir las interceptaciones telefónicas por vulnerar las expectativas razonables de privacidad en estos canales cerrados de comunicación. Posteriormente, en 1979 (*Smith c. Maryland*), la Corte precisó que esa protección no se extendía a los números marcados de un teléfono a otro, pues, al ser entregada voluntariamente esa información por los titulares a la empresa de telefonía para la conexión, el titular habría renunciado a su carácter de reservado.

Por lo anterior, en ese sistema se entiende que el Estado se encuentra legitimado para requerir al tercero que administra el canal de comunicación, aquellos datos o elementos del proceso de comunicación que no permanecieron en la esfera exclusiva de los comunicantes. Así, la empresa de telefonía está obligada a proporcionar, a las autoridades competentes, información a la policía sobre qué números se comunicaron entre sí, con qué frecuencia, en qué fechas, entre otros elementos que den cuenta de la existencia de procesos de comunicación.

En contraste con ello, el artículo 8.1 del CEDH reconoce que “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su **correspondencia**”. Por eso, el TEDH estima que la protección de las comunicaciones es parte del derecho a la vida privada, y esa reserva abarca a todos los elementos del proceso de comunicación, sin importar el carácter íntimo de lo comunicado. El TEDH consideró lesivo de la vida privada la práctica de la policía británica que requería información de la oficina postal sobre el registro de números marcados de ciertos

teléfonos, el tiempo y duración de cada llamada. Por ende, si bien no se accede a la información transmitida, sí a los elementos que dan cuenta de la existencia de un proceso de comunicación, lo que está protegido por la expectativa del secreto de las comunicaciones (Malone, 1984, pp. 83-88). Gracias al TEDH, en Europa la información que se facilita a quien administra y hace posible el proceso de comunicación (servicio postal, empresa de telefonía o de internet) está protegida por el derecho al secreto, el cual abarca a todo este proceso y sus elementos⁷.

También la Corte Constitucional italiana, en el fundamento tercero del asunto Sentencia 366/1991, recurrió a una interpretación extensiva de los derechos fundamentales para proclamar que el derecho al secreto protege al proceso de comunicación, a lo comunicado y a los elementos del proceso de comunicación. En virtud de ello, en el fundamento cuarto del asunto Sentencia 81/1993, la Corte concluyó que este derecho:

[...] implica la seguridad de que el titular [...] puede elegir libremente los medios de comunicación, también las diferentes condiciones que aseguren la confidencialidad tanto desde el punto de vista técnico como jurídico [...] debe reconocerse el derecho a mantener en secreto tanto los datos que puedan conducir a la identificación de los sujetos de la conversación como los relativos al momento y lugar de la comunicación. [traducción libre]

Desde esta perspectiva, es razonable que el derecho al secreto genere obligaciones que excluyan a los terceros de conocer la existencia misma del proceso comunicativo, pero más importante todavía, es razonable que exista un deber especial sobre el administrador o facilitador del canal cerrado de comunicación que, a diferencia del régimen estadounidense, sí tendrá que guardar confidencialidad. La Corte Constitucional italiana, en el fundamento cuarto del asunto Sentencia 81/1993, señala que:

[...] no se puede negar que el reconocimiento de tal derecho está co-esencialmente ligado con la garantía consistente en el deber que recae sobre aquellos que por razones profesionales conocen el contenido y los datos externos de la comunicación, de mantener la más estricta confidencialidad sobre los elementos que se acaban de mencionar. Si esa garantía no

⁷ La relación entre comunicantes y facilitador del proceso no será analizada aquí, pues tiene un régimen especial que les habilita para el acceso, manejo y uso de ciertos datos del tráfico de la información, sin lesionar el derecho al secreto. En lo sucesivo, solo nos referiremos a las hipótesis frente a otros terceros que deben ser totalmente ajenos a ese proceso, pero pretenden interferir o acceder a él, lo que sí podría atentar contra el derecho analizado.

existiera, se frustraría el contenido del derecho [...] se intenta garantizar [...] más aún si este implica para su realización la intervención de ciertos medios y de hombres. [traducción libre]

En nuestra región, la Corte Interamericana de Derechos Humanos (en adelante, CIDH) considera también que la protección sobre las comunicaciones reservadas debe abarcar a todos los elementos del proceso de comunicación, como el destino de la comunicación, el origen, la identidad de interlocutores, la frecuencia, la hora y la duración. Aunque la CIDH hace referencia únicamente a la intervención sobre llamadas telefónicas, al igual que el TEDH, no debería tener problemas en aplicar un criterio similar a las actuales técnicas de comunicación, en el que concurren otros elementos (metadatos) en el proceso comunicativo⁸.

En suma, si lo que se pretende es proteger es el secreto del proceso de comunicación y no solo la privacidad o reserva de lo que se comunica, solo se arribará a este objetivo protegiendo todos los elementos de ese proceso de comunicación, ya que si los terceros conocen u obtienen dichos elementos se quebrantará el secreto que se pretendía establecer sobre la existencia misma de dicho proceso.

C. Elementos estáticos y dinámicos del proceso de comunicación

Hemos dejado claramente establecido que el derecho al secreto protege la irrupción de terceros sobre comunicaciones en curso y sobre sus elementos, pero es necesario profundizar qué sucede con los elementos estáticos del proceso de comunicación, como el aparato de comunicación o el número de identificación de este. En las líneas sucesivas desarrollaremos si corresponde o no proteger el mensaje recibido y almacenado en alguna base de datos personales o en plataformas de acceso reservado.

El derecho al secreto protege a todos los elementos vinculados con un proceso de comunicación, empero, no protege datos estáticos como un número telefónico, el número de serie de una computadora, etc. No es que estos elementos carezcan de tutela alguna, sino que la protección de estos elementos se efectiviza a través del derecho a la privacidad y no por el derecho al secreto. Este último derecho protege los elementos estáticos en tanto y en cuanto estén vinculados con un proceso de comunicación específico, que se extenderá frente a toda interrupción o intervención de un

proceso comunicativo, o frente a todo intento por acceder a los elementos o la información misma de una comunicación en curso.

Desde hace veinte años, el Tribunal Supremo y el TC español vienen consolidando una línea jurisprudencial que indica, por ejemplo, que el acceso a la agenda de números telefónicos, o de números que aparecen en la lista de contactos no se encuentran protegidos por el derecho al secreto (STS 1315/2009; STS 169/2011; STS 321/2011; SENTENCIA 142/2012, fundamentos 3-4 y SENTENCIA 115/2013, fundamentos 3-4), aunque, en determinadas circunstancias, podrían ser tutelados por el derecho a la privacidad. En ese sentido, tampoco consideran que sean merecedoras de protección por el derecho al secreto, la identificación de los números telefónicos de los investigados (STS 901/2009, STS 362/2011, STS 83/2013), ni el acceso a los datos de identidad internacional de un celular como el *International Mobile Equipment Identity* (IMEI) o *International Mobile Subscriber Identity* (IMSI) (STS 79/2011; STS 249/2008; STS 686/2013) o a la identidad críptica de una computadora o IP (STS 842/2010; STS 739/2008; STS 680/2010).

Los tribunales españoles advierten que, si bien se podría tratar de información sensible o reservada, bajo el derecho a la intimidad, en sí misma no son formen parte de un proceso comunicativo y, por ende, no son merecedoras de protección bajo el derecho al secreto. En suma, los elementos estáticos utilizados en un proceso de comunicación por sí solos no son pasibles de protección por el derecho al secreto.

No obstante, debido a la interacción entre ambos espacios, será difícil actuar sobre uno sin alterar al otro. Por ejemplo, acceder a archivos de una computadora podría vulnerar tanto la intimidad como el secreto de las comunicaciones, al exponer información privada o elementos de un proceso comunicativo.

Esta dificultad ya fue abordada por la Corte Suprema de los Estados Unidos en el caso Riley, donde señaló que un teléfono celular es una suerte de minicomputadora. Entre sus funciones están realizar llamadas y formas de comunicación, así como almacenar información que no es parte de un proceso de comunicación (fotos, historial de navegación por internet, documentos, entre otros). La Corte consideró que todos estos contenidos se encuentran protegidos por el derecho a la privacidad (recuerden que no lo distinguen del secreto

⁸ Véase el caso Escher, Sentencia de 6 de julio de 2009, párrafo 114. En nuestro país, ver el caso Alberto Quimper, Expediente 0655-2010-HC, fundamentos 18-19.

de las comunicaciones), por lo que su acceso exige consentimiento del titular o mandato de un juez⁹.

En el Perú, la protección del proceso de comunicación solo abarca los elementos directamente vinculados con dicho proceso. Ninguna interpretación razonable permitiría extender su alcance a elementos estáticos que podrían —o no— ser usados en procesos de comunicación (como computadoras, celulares, números de teléfono, entre otros). En tales casos, corresponderá aplicar la tutela del derecho a la privacidad.

Existe consenso en el TC español, TC alemán, la Corte Constitucional italiana, el TEDH y la CIDH en que el secreto de las comunicaciones protege a todos los elementos que forman parte o dan cuenta de un proceso de comunicación. Además, el TC peruano, en el caso denominado Alberto Quimper ha recogido estos criterios y ha resaltado que este derecho protege:

[...] cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones. (Expediente 0655-2010-HC, fundamento 18)

Por lo tanto, no cabe duda de que, incluso al acceder a datos vinculados a procesos de comunicación ya concluidos, deben aplicarse las garantías de legalidad y mandato judicial que prevé el artículo 2 numeral 10 de la Constitución, como requisito para toda intervención en el secreto de las comunicaciones.

D. El contenido del proceso de comunicación

El TC español ha determinado que el acceso de terceros al registro de llamadas telefónicas constituye vulneración del secreto de las comunicaciones, al revelar la existencia de procesos comunicacionales (Sentencia 123/2002; Sentencia 230/2007; Sentencia 142/2012; Sentencia 173/2011). No obstante, dicho estándar no aplica cuando uno de los intervinientes en la comunicación faculta a un tercero para

acceder al proceso comunicativo o sus elementos. Sobre esta hipótesis, el TC peruano, en su fundamento cuarto del Expediente 0867-2011-AA, denominado caso Alan Quintano, ha establecido que:

[...] resulta preciso distinguir entre el proceso de la comunicación y el contenido de la comunicación. El primero [protegido por el derecho al secreto] [...] prohíbe cualquier injerencia externa por parte de un tercero... El segundo no impone un deber de reserva o de secreto de lo comunicado por el solo hecho de haber recibido o entrado en la comunicación. Ello es así porque, en tal supuesto, solo si el contenido de la comunicación fuera difundido o transmitido a terceros, esa actuación tal vez puede suponer, según sea el caso, la afectación del derecho a la intimidad personal o familiar, pero no la afectación del derecho al secreto de las comunicaciones.

En el caso citado, al ser uno de los interlocutores quien grabó la llamada recibida, el registro fue considerado bajo el ámbito del derecho a la intimidad y no como la interferencia de un tercero en el secreto de las comunicaciones. Es decir, no existió vulneración de este derecho, pues no hubo interceptación por un tercero, sino que fue un participante quien: (i) facilitó el acceso a un tercero al contenido comunicado; o (ii) grabó y posteriormente compartió dicha comunicación. Por tanto, es posible que uno de los comunicantes permita a terceros acceder a mensajes de texto, correos electrónicos, o a todo tipo de comunicaciones realizadas por canales cerrados, sin que ello configure vulneración del secreto de las comunicaciones. No obstante, dicha conducta podría representar una afectación al derecho fundamental a la privacidad¹⁰.

Si uno de los comunicantes no autoriza a un tercero, el TC peruano considera que el derecho al secreto mantiene una eficacia inalterable y, además, alcanzará a todo el proceso de comunicación e incluso a la comunicación recibida, leída y archivada. Es decir, protege lo comunicado, sea que forme parte de un proceso de comunicación en curso, o que esté almacenado en algún sistema o archivo. En este asunto, nuestro sistema de derechos difiere de los criterios adoptados por el TC español y alemán. Estos tribunales consideran que el secreto protege el proceso de comunicación en curso y a

⁹ Este mismo criterio de la jurisprudencia comparada ha sido aplicado por la Corte Superior de Justicia del Callao, por lo que ha considerado que cualquier acceso no autorizado al celular, requiere de autorización judicial para ser legítimo (caso Emiliano Mucha Lagos y otros, fundamentos 3.15 a 3.19).

¹⁰ En un caso donde uno de los interlocutores grabó una conversación que daba cuenta de un supuesto ilícito, la instancia inferior había excluido la prueba por estimarla lesiva del derecho al secreto de las comunicaciones. Sin embargo, en línea con el criterio de nuestro TC y del TC español (Sentencia 56/2003), la Sala Penal Transitoria de la Corte Suprema anuló ese fallo al considerar que en tal caso no existía intervención de un tercero sobre la conversación, ni un agravio contra el secreto de las comunicaciones. Véase el caso Doig Sánchez, Resolución del 26 de abril de 2016, recurso de nulidad, de la Sala Penal Transitoria de la Corte Suprema y el Expediente 2076-2014, fundamento 6.

sus elementos, pero luego de finalizado el proceso comunicativo, sostienen que la información recibida solo estaría protegida por la intimidad y no por el derecho al secreto de las comunicaciones¹¹.

En efecto, el TC peruano ha atendido este asunto en los casos en los que se accede sin autorización a procesos de comunicación realizados por trabajadores a través de cuentas de correo, mensajería o teléfonos facilitados por su empleador. En estos casos, el empleador accedió a los mensajes electrónicos de sus trabajadores para usarlos como pruebas de uso indebido de los bienes facilitados por la empresa y, por ende, como causal de despido. Sin embargo, el TC consideró que el derecho al secreto alcanzaba tanto al proceso de comunicación, como a la información recibida y archivada en las computadoras o celulares facilitada por la empresa¹².

Es decir, el TC y la Corte Suprema peruana consideran que se vulnera el derecho al secreto cuando un tercero accede a un proceso de comunicación en curso (y sus elementos) o cuando ni siquiera interrumpe ese proceso (ni conoce de su existencia), sino que accede a la comunicación entregada, revisada y archivada, tal como lo hacen su pares españoles y alemanes (Sindicato Único de Trabajadores de Nestlé Perú, Casación 14614-2016-Lima, fundamento 18). Para el TC peruano, todo eso (proceso, elementos y comunicación archivada) están protegidos por el derecho al secreto.

Tal vez podría interpretarse que la postura del TC peruano pretende sustentarse en un argumento lingüístico, aunque paradójicamente, no ha sido muy explícito en su lenguaje. Y es que el texto constitucional proscribire 'abrir' o 'incautar' comunicaciones o telecomunicaciones, acciones que solo pueden usarse respecto de contenidos almacenados o grabados y no de procesos de comuni-

caciones en curso (salvo los casos de cartas). Por ejemplo, un telegrama, una llamada telefónica o electrónica, una videollamada, o un correo electrónico, solo podrán 'incautarse' o 'abrirse' si sus contenidos se encuentran almacenados o grabados en algún lugar.

Eso indicaría que en el Perú existe un mandato constitucional expreso para que el derecho al secreto alcance al proceso de comunicación y al contenido almacenado de aquello que se comunicó, tal como lo ha entendido el TC.

E. El secreto de las comunicaciones de los trabajadores

El TC peruano aún no define claramente qué ocurre cuando los canales de comunicación son administrados o facilitados por la empresa a sus trabajadores y, respecto de los cuales, se indica expresamente que no serán canales privados, sino de acceso para el empleador. Todavía no queda claro si tales canales merecen protección bajo el derecho al secreto. A diferencia del TEDH en el caso Barbulescu (sentencia del 5 de septiembre de 2017), el TC peruano tampoco ha evaluado si los canales de comunicación cerrados, sobre los que no cabe una 'expectativa razonable de privacidad', merecen o no protección por el derecho al secreto.

El reciente caso Paucarcaja Mercado, recaído en el Expediente 0943-2016-AA, fue una buena oportunidad para esa precisión, pero no se concretó. El TC peruano declaró improcedente una demanda de amparo en la que se discutía el despido de un trabajador por una falta grave, acreditada mediante el acceso del empleador al correo de Facebook que este había abierto usando equipos de la empresa. El voto minoritario consideró que debía declararse fundada la demanda, invocando los cri-

¹¹ Tiene dicho el TC español que:

Esta doctrina ha sido reiterada recientemente en la Sentencia 70/2002 [...] precisamos que [...] la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos, de modo que la protección de este derecho alcanza a las interferencias habidas o producidas en un proceso de comunicación. La separación del ámbito de protección de los derechos fundamentales a la intimidad personal... y al secreto de las comunicaciones [...] efectuada en esta Sentencia se proyecta sobre el régimen de protección constitucional de ambos derechos. Pues si [...] la intervención de las comunicaciones requiere siempre resolución judicial, 'no existe en la Constitución reserva absoluta de previa resolución judicial' respecto del derecho a la intimidad personal [...]. (Sentencia 123/2002, fundamento 4)

El desarrollo de la jurisprudencia alemana lo veremos con mucho mayor detalle más adelante.

¹² Véase los Casos Rafael García (Expediente 1058-2004-AA), Laura Vizquerra (Expediente 5532-2014-AA) y Ángela Huamaní (Expediente 4224-2009-AA). En este último caso, el TC precisó que:

[...] si bien la fuente o el soporte de determinadas comunicaciones y documentos le pertenecen a la empresa o entidad en la que un trabajador labora, ello no significa que ésta pueda arrogarse en forma exclusiva y excluyente la titularidad de tales comunicaciones y documentos, pues con ello evidentemente se estaría distorsionando el esquema de los atributos de la persona, como si estos pudiesen de alguna forma verse enervados por mantenerse una relación de trabajo.

terios del caso Barbulescu del TEDH y la jurisprudencia española para sostener que:

[...] no es posible sostener una prohibición absoluta por parte del empleador para fiscalizar el contenido de las conversaciones del trabajador si es que utiliza un medio tecnológico otorgado por la empresa como es el correo electrónico institucional. El mismo TC español ha reconocido el acceso empresarial a los correos del trabajador si es que se logra superar el juicio de proporcionalidad (Sentencia 170/2013), siempre y cuando se trate de una medida ponderada y equilibrada que cumpla con los siguientes criterios:

- El control empresarial ha de realizarse con garantías (por ejemplo: a través de la intervención de perito informático y notario).
- El contenido de los mensajes no ha de reflejar aspectos específicos de la vida personal y familiar del trabajador, sino únicamente información relativa a la actividad empresarial, cuya remisión a terceros implique una transgresión de la buena fe contractual.
- De tal forma que, atendida la naturaleza de la infracción investigada y su relevancia para la entidad, no pueda apreciarse que la acción empresarial de fiscalización haya resultado desmedida respecto a la afectación sufrida por la privacidad del trabajador.

Por lo tanto, este Tribunal debe reconocer la facultad del empleador de fiscalizar e intervenir en el correo electrónico institucional si es que previamente ha comunicado al trabajador tanto de la posibilidad de la monitorización de sus comunicaciones a través de este medio, así como de las condiciones de uso permitido por la empresa. (fundamentos 28-29)

Aunque se trata de un voto minoritario, se observa que el TC empieza a mostrar una tendencia a flexibilizar la posibilidad de que un tercero, como el empleador, acceda (o fiscalice) el uso de las herramientas tecnológicas que proporciona a sus trabajadores. Por ahora, lo único claro es que el TC peruano está obligado a otorgar un alcance más amplio al derecho al secreto que sus pares españoles y alemanes, ya que una interpretación literal del texto constitucional exige que este derecho proteja no solo el proceso de comunicación y sus elementos, sino incluso lo comunicado y archivado.

En ese aspecto, nuestra jurisprudencia parece aproximarse más a los criterios de la Corte Suprema francesa, que ha sido especialmente abundante en esta materia. Por ejemplo, en el caso Nikon, estableció que:

[...] el empleador no puede, por lo tanto, sin violar esta libertad fundamental [del secreto de las comunicaciones], tomar conocimiento de los mensajes personales enviados por el empleado y recibidos por él gracias a una herramienta informática puesta a su disposición para sus trabajos, incluso si el empleador hubiera prohibido el uso no profesional de la computadora. (2001) [traducción libre]

Este criterio ha sido ratificado poco después en el caso Sulzer en donde se estableció que “el trabajador tiene derecho, incluso en la hora y el lugar de trabajo, a respetar la reserva de su vida privada; que esto implica en particular el secreto de la correspondencia¹³”.

Posteriormente, en el caso Nycomed, la Corte Suprema francesa precisó su jurisprudencia al examinar el despido de un empleado en cuyo cajón del escritorio se encontraron fotografías eróticas, lo que llevó al empleador a revisar su computadora y archivos marcados como ‘personales’, donde halló más imágenes. El máximo tribunal francés determinó la invalidez del despido por considerarlo una violación del derecho a la privacidad, aunque estableció que este tipo de intervención patronal podría ser válida bajo cuatro condiciones: (i) que exista un reglamento interno que autorice expresamente este control; (ii) que el trabajador esté presente o debidamente convocado durante la revisión; (iii) que medien circunstancias excepcionales que justifiquen la medida; y (iv) que se evalúe proporcionalmente la intensidad de la intervención según el grado de acceso (libre o restringido) a los archivos revisados¹⁴.

Y en el caso Bianchi, la Corte Suprema delimitó aún más dicha intervención: al revisar el despido de una trabajadora por tener tres latas de cerveza en su espacio personal, estableció que las intromisiones patronales en áreas reservadas solo son válidas “si están justificadas por la naturaleza de las tareas que se realizan y en proporción al fin buscado, en donde especialmente el empleador puede realizar [tales intervenciones]¹⁵” [traducción libre]. En el caso Sanofi se aplicó un criterio similar, reconociendo como legítima la intervención de correos

¹³ Cámara Social, 2 de octubre de 2001, 99-42.942.

¹⁴ Cámara Social, 17 de mayo de 2005, 03-40.01.

¹⁵ Cámara Social, 11 de diciembre de 2001, 99-43.030

electrónicos y archivos personales, pero únicamente si: (i) se delegaba dicha revisión a un órgano que asegurara la confidencialidad de los datos personales; y (ii) la investigación se circunscribía exclusivamente a los riesgos comerciales que motivaban la intervención¹⁶.

Sin duda, el desarrollo del derecho a la privacidad y al secreto de las comunicaciones en el ámbito laboral plantea más problemas de los que podemos analizar aquí¹⁷. Por ahora, el TC peruano muestra una tendencia que favorece la protección de los derechos laborales, sin negar por ello el poder de dirección empresarial. No obstante, nuestra jurisprudencia aún no aborda todos los escenarios posibles en esta relación laboral.

El TC peruano ha extendido estos criterios más allá del ámbito laboral privado. En el caso denominado Victoria Contreras, signado bajo el Expediente 3901-2007-AA, declaró improcedente la sanción impuesta por la Marina de Guerra a una cadete por mantener una relación sentimental, basada en mensajes de texto –actuales y archivados– obtenidos mediante el acceso a su celular por parte de un superior. El TC sostuvo que dichos contenidos estaban protegidos por el secreto de las comunicaciones, confirmando que esta garantía abarca tanto el proceso comunicativo como su contenido archivado (fundamentos 25-30)¹⁸.

En resumen, en el Perú el derecho al secreto de las comunicaciones procura la confidencialidad de todo el proceso de comunicación, como el hecho de su existencia. Esta protección jurídica se extiende necesariamente a todos aquellos elementos. Es decir, el ordenamiento jurídico protege estos elementos en la medida exacta en que pueden servir para evidenciar la existencia de un proceso comunicativo que, por haberse realizado a través de canales cerrados, estaba destinado a permanecer en el ámbito de lo reservado. Por tanto, no debe sorprendernos que dentro de esos elementos dinámicos se proteja la identidad de los comunicantes, de los aparatos de comunicación que se usan, la ubicación o la geolocalización de los celulares¹⁹ o de los terminales electrónicos empleados, la fecha, hora, cantidad, contenido o cualidad de la información transmitida, así como los datos de tráfico usados para poder realizar la conexión de teléfonos o de los canales electrónicos de comunicación (y es que, para conectar llamadas telefónicas o comunicaciones electrónicas, se necesitan otros elementos que son los que permiten la administración, direccionamiento y control de los procesos de comunicación).

Efectivamente, para garantizar dicha reserva del proceso comunicativo, resulta indispensable proteger igualmente el contenido transmitido, ya se encuentre en tránsito o almacenado.

¹⁶ Cámara Social, del 17 de junio de 2009, 08-40.274

¹⁷ Peyrat-Guillard hace un excelente resumen sobre la relación trabajador-empleador:

[...] hay buenas razones para monitorear el comportamiento de los trabajadores. De hecho, la vigilancia se implementa dentro de las empresas no solo para mejorar el rendimiento o la productividad, sino también como protección contra los riesgos [...] que el comportamiento de los empleados pueda cometer contra el empleador, el público [...] sus colegas o ellos mismos. Por lo tanto, [se pueden] distinguir tres tipos de justificaciones para la vigilancia: los intereses del empleador [...], los intereses del trabajador y los intereses de terceros, como clientes o compañeros de trabajo... la vigilancia debe justificarse en relación con los intereses de uno u otro y, según el objetivo, siempre debe favorecerse el dispositivo menos intrusivo. Por lo tanto, el monitoreo puede estar justificado en ciertas circunstancias en relación con este doble objetivo de proteger y mejorar los resultados. Puede, por ejemplo, tener como objetivo garantizar la protección de quienes trabajan en contextos peligrosos, para evitar el robo o el fraude, o incluso para mejorar la calidad de los productos y servicios, pero no debe, sin embargo, contravenir el respeto de la vida privada [...] En cada caso se debe considerar los elementos que concurren, por ejemplo, se señala, que "si los mensajes de trabajo pueden enviarse por la noche, los fines de semana o durante las vacaciones, esto brinda argumentos para considerar que también pueden enviarse mensajes personales durante el horario laboral... al definir su política laboral, el empleador debe tener en cuenta la necesidad de los trabajadores de resolver asuntos personales desde su lugar de trabajo. La línea entre la vida profesional y la privada se verá borrosa debido al acceso a internet a menudo más eficiente en la oficina o a la necesidad de terminar el trabajo en casa, lo que ya permite saber con certeza cuándo termina la jornada laboral [...]". (2012, p. 155)

¹⁸ El mismo criterio asume la Corte Superior de Justicia de Lima en el caso Jorge Acurio, (Resolución del 28 de marzo de 2018 [auto de apelación], de la Sala Penal de Apelaciones, Colegiado A, de la Corte Superior de Justicia de Lima, Expediente 11-2017, fundamento 6.2), citamos:

Este derecho fundamental protege cualquier comunicación con independencia de su contenido, pertenezca o no al ámbito de lo personal, íntimo o reservado, pues existe una presunción iuris et de iure de que lo comunicado es secreto. Esta protección constitucional no solo se limita al contenido de la comunicación, sino al soporte de la misma y a las circunstancias que rodean todo el proceso comunicativo, cualquiera sea la técnica utilizada.

¹⁹ Cabe insistir que, nos referimos a la geolocalización del celular (y a los demás elementos) durante un proceso comunicativo. Fuera de eso, la sola ubicación del celular no corresponde al derecho al secreto. Ese dato cae bajo el ámbito de protección del derecho a la privacidad, en la medida que se mantiene una 'expectativa razonable de privacidad'. Esa es la línea que asume nuestro Decreto Legislativo 1182 (y sus modificaciones) que regula el acceso policial a la geolocalización. Y a nivel comparado, esa línea es sostenida por la Corte Suprema de Estados Unidos en *Carpenter* contra Estados Unidos (138 S.Ct. 2206) de 2018. Véase a Freiwald y Smith (2018, p. 205 y siguientes) y Rozenshtein (2019, p. 943 y siguientes).

VI. CARACTERÍSTICAS DEL PROCESO DE COMUNICACIÓN PROTEGIDO

El proceso de comunicación protegido por el derecho al secreto debe cumplir dos requisitos fundamentales: (i) haber sido realizado mediante ‘canales facilitados o brindados por terceros’ distintos a los comunicantes; y (ii) tratarse de ‘canales cerrados de comunicación’ con interlocutores determinados que cuenten con expectativas razonables de privacidad.

A. Procesos de comunicación facilitados por terceros

La jurisprudencia alemana sentó los criterios fundamentales posteriormente adoptados en nuestro sistema. El TCF precisa que el derecho al secreto opera cuando existe separación física entre los interlocutores, lo que los obliga a utilizar medios externos para transmitir mensajes confidenciales. Durante este proceso, carecen de control sobre la seguridad y confidencialidad de sus comunicaciones, a diferencia de lo que ocurre en interacciones directas. Precisamente ante esta imposibilidad de garantizar la reserva, el ordenamiento jurídico establece salvaguardias para prevenir intromisiones indebidas²⁰. Por eso indica que el derecho al secreto:

[...] se asocia con una pérdida de privacidad, porque los comunicadores tienen que involucrarse en las peculiaridades técnicas de un medio de comunicación y confiar en involucrar a un intermediario de la comunicación. De este modo, el contenido y las circunstancias de la transmisión del mensaje están expuestos a un acceso más fácil por parte de terceros. Las partes que se comunican a distancia con ayuda de técnicas de enlace externo no tienen la opción de garantizar la confidencialidad de su comunicación [Por eso, el derecho] tiene por objeto compensar la pérdida de privacidad por razones técnicas y contrarrestar los peligros que surgen del proceso de transmisión, incluida la participación de un tercero. (BVerfGE 115, 166; BVerfGE 85, 386; y BVerfGE 106, 28) [traducción libre]

Esto explica la razón por la cual el derecho al secreto protege exclusivamente los procesos comunicativos administrados por terceros: únicamente en estos casos los interlocutores carecen de capacidad para controlar o resguardar los elementos transmitidos, delegando dicha protección a un tercero. Dado que la comunicación debe recorrer una distancia física, los titulares del derecho no disponen de mecanismos para prevenir su interceptación o alteración durante la transmisión, dependiendo completamente del proveedor del servicio. Esta pérdida de autonomía sobre ámbitos privados fundamenta la necesidad de otorgar protecciones reforzadas: “La protección especial del secreto de las telecomunicaciones [...] compensa la pérdida técnica de la capacidad de control de la privacidad, que surge inevitablemente mediante el uso de sistemas de terceros” (BVerfGE 115, 166)²¹.

Ese razonamiento les llevó a sostener que la protección del secreto solo rige durante la ejecución del proceso comunicativo, pues es en esta fase cuando los interlocutores carecen de control y están expuestos a riesgos de interceptación. Concluido el acto comunicacional, la información recibida y almacenada queda amparada exclusivamente por el derecho a la intimidad, en la medida que los sujetos conservan la facultad de destruir o mantener en reserva lo transmitido (BVerfGE 115, 166; BVerfGE 120, 274).

Estos criterios se desarrollaron para comunicaciones tradicionales (cartas, telegramas, teléfonos fijos), donde el destinatario podía eliminar los rastros de lo comunicado. Las comunicaciones electrónicas, en cambio, generan huellas persistentes incluso después de finalizado el acto comunicativo, imposibilitando a los sujetos eliminar todos los datos de tráfico y garantizar su reserva. Esta eliminación resulta técnicamente compleja, costosa o inviable incluso para los administradores del servicio. En un caso sobre acceso a correos electrónicos, el TCF constató que la información se almacenaba tanto en el dispositivo del usuario como en los servidores del proveedor, sin que los interlocutores tuvieran capacidad técnica para impedir dicho acceso. Ante esto, el TCF determinó que el

²⁰ Gusy señala que:

[...] sólo [sic] las comunicaciones individuales están sujetas a la protección del secreto de las telecomunicaciones, es decir, la comunicación mediada electrónicamente, que se dirige únicamente a un destinatario o a un grupo limitado de destinatarios previamente determinado individualmente (como una conferencia telefónica) [...] Su contraparte legal es la radiodifusión, que se dirige al público en general y, por lo tanto, no reclama ni disfruta de protección de confidencialidad. (2018, párrafo 64)

²¹ El TC español sigue esta postura. Véase las Sentencias 123/2002, fundamento 5 y 170/2013, fundamento 4 [...], pero en Italia la Corte Constitucional estima que el derecho al secreto protege todo tipo de procesos de comunicación, incluso las realizadas directamente entre hablantes, siempre que exista ‘expectativas razonables de privacidad’ (Sentencia 135/2002, fundamento 3 y Sentencia 148/2008, fundamento 4).

derecho al secreto debe extenderse a la información almacenada por el proveedor, incluso concluida la comunicación (BVerfGE 124, 43). Este mismo fundamento se aplica a comunicaciones telefónicas y digitales, pues al carecer los usuarios de medios para eliminar los datos de tráfico, el tribunal extendió la protección del secreto a estos elementos (BVerfGE 67, 157; BVerfGE 85, 386; BVerfGE 110, 33; BVerfGE 115, 166).

En suma, el TCF reconoce que el derecho al secreto protege todos los elementos del proceso comunicativo, pero únicamente cuando constituyan evidencia de una comunicación reservada que el titular no pueda eliminar. Este criterio es compartido por la jurisprudencia española. En cambio, el TC peruano protege: (i) el proceso comunicativo; (ii) sus elementos constitutivos; (iii) el contenido transmitido; y (iv) sus rastros digitales, sin condicionar dicha protección a la posibilidad técnica de eliminación de los datos por parte de los participantes.

En efecto, el artículo 2.10 de la Constitución indica que el derecho al secreto protege las comunicaciones entre sujetos separados espacialmente, al prohibir específicamente su ‘intercepción’ e ‘intervención’, que solo es posible cuando las personas están separadas y deben recurrir a un canal que pueda ser interceptado o intervenido. Asimismo, la norma constitucional prohíbe el ‘abrir’ e ‘incautar’ comunicaciones, lo que demuestra que la tutela jurídica abarca tanto la protección contra interferencias en procesos comunicativos activos, como la garantía de reserva sobre dichos procesos y las comunicaciones almacenadas potencialmente accesibles.

B. Procesos de comunicación realizados por canales cerrados

La protección jurídica no se extiende a toda comunicación que los interlocutores pretendan mantener en reserva, sino únicamente a aquellas que utilicen canales técnicos proporcionados por

terceros, diseñados específicamente para garantizar la confidencialidad del proceso comunicativo²². Piénsese en los terceros que brindan el servicio postal, en una compañía de teléfonos, o en una transmisión de datos o de internet. Por lo tanto, la conversación directa entre las personas²³, las realizadas a través de canales de señal abierta (radio, televisión, *walkie talkie*) o, incluso las comunicaciones con canales cerrados, pero sin ‘expectativa razonable de secreto’ (como llamadas telefónicas a centrales de emergencia, a programas de señal abierta) no serán objeto de protección del secreto de las comunicaciones.

En un caso en donde se entregó correspondencia abierta, sin un sobre, ni sello de reservado, secreto u otro análogo, no puede existir ‘expectativa razonable de privacidad’ bajo el derecho al secreto de las comunicaciones²⁴. En el caso Jackson de 1877, la Corte Suprema de Estados Unidos precisó que los correos no sellados como periódicos, panfletos o revistas están abiertos a cualquier inspección, pues no se espera reserva respecto de ellos. En el caso B.C. (párrafo 1) la Comisión Europea de Derechos Humanos negó que la interceptación y grabación de conversaciones que usaban ondas de telecomunicación no reservadas, indicara que sus intervinientes aceptaban el riesgo de que sean detectadas y reveladas.

En los casos Halford (sentencia del 27 de junio de 1997), Copland (sentencia del 3 de abril de 2007) y Amann (sentencia del 16 de febrero del 2000), el TEDH precisó que, si bien una persona puede estar en un espacio público (centro comercial, oficina pública) eso no significa que carezca del derecho al secreto de comunicaciones, pues este se relaciona con el uso de canales cerrados para comunicarse con otro (telefónico o electrónico), con independencia de donde esté el acceso a dicho canal. El uso de vías cerradas genera la expectativa razonable de secreto sobre el proceso comunicación, eso lo que justifica su protección. Por ejemplo, un teléfono ubicado en una dependencia policial y usado por

²² Pagenkopf se refiere a la jurisprudencia alemana para señalar que:

El ámbito de protección del derecho fundamental al secreto de las telecomunicaciones sólo [sic] puede abrirse si existe una comunicación establecida, objetivamente protegible y segura. De esa protección de la confidencialidad se deduce que algo no cabe allí si no sirve para comunicarse en absoluto o sólo es un canal imperfectamente confidencial desde un punto de vista técnico y objetivo. Esto significa que cualquier medio que sea técnicamente vulnerable e imperfecto, que corresponda básicamente a una comunicación pública, con posibilidad general de participación, queda fuera del ámbito de protección. Debe tratarse de una vía de transmisión «encubridora», es decir, “oculta”, “secreta” que pueda protegerse [...] El ordenamiento jurídico no puede calificar de secreto un grito que es audible para todo el mundo, más que un sistema completamente abierto electrónicamente. (2021, párrafos 14.b y 14.c)

²³ Según las circunstancias, esas conversaciones directas entre las personas podrían ser pasibles de tutela en virtud del derecho a la intimidad. Y es que, a pesar de darse en lugares abiertos, tienen expectativas razonables de privacidad, por lo que en los casos Bigaeva (Sentencia del 28 de mayo de 2009) y Özpinar (Sentencia del 19 de octubre de 2010), el TEDH reconoce que la intimidad alcanza la ‘vida social privada’ entendida como posibilidad de que el individuo desarrolle libremente su identidad social sin que sea posible seguimientos constantes.

²⁴ Véase a la Corte Superior de Justicia de Ancash, Expediente 45-1997, caso Jorge Acurio.

una funcionaria, o en un centro de trabajo y usado por un empleado, no pueden ser intervenido porque, en las circunstancias del caso, generan ‘expectativas razonables de privacidad’ del proceso de comunicación (Halford, párrafo 43-46 y Copland, párrafo 42). Lo que indica que la expectativa del secreto recae sobre todo el proceso de comunicación, la protección de esos espacios es lo que asegura la libertad de la comunicación transmitida²⁵.

En el caso Barbulescu, el TEDH reconoció que la ‘expectativa razonable de privacidad’ sobre los procesos de comunicación es uno de los elementos que define su protección, y en los casos Perry y López Ribalda usó el mismo criterio para identificar espacios protegidos por el derecho a la intimidad (recuérdese que el TEDH extiende una única protección sobre ambos derechos).

En conclusión, el derecho al secreto garantiza la reserva tanto del proceso comunicativo en sí como de su existencia, lo que implica necesariamente la protección de todos sus elementos constitutivos –incluyendo el contenido mismo de la comunicación, cuya naturaleza resulta irrelevante para efectos de su amparo–. Sin embargo, dicho derecho solo protege aquellos procesos comunicativos que cumplen con dos requisitos esenciales: (i) la utilización de canales proporcionados y administrados por terceros; y (ii) el empleo de canales cerrados que generen expectativas razonables de privacidad.

Como se protege todo proceso de comunicación sin importar la naturaleza de su contenido, lo distintivo del derecho se encuentra en el tipo de canal al que se refiere este derecho, cuyas características pueden ser graficadas así:

Gráfico 2: Proceso de comunicación protegido



Fuente: Elaboración propia

Los elementos anteriores, permiten advertir los errores del TC al analizar el caso Víctor Polay Campos (Expediente 0774-2005-HC, fundamento 24), ya que aplicó el derecho al secreto de las comunicaciones cuando lo que correspondía era aplicar el régimen del derecho a la intimidad. En ese caso, se cuestionaba el acceso a las conversaciones entre abogado y patrocinado en el locutorio penitenciario (en donde los hablantes se ven directamente y están separados por un material transparente) y en las entrevistas directas que estos tenían. Tales situaciones caerían bajo la protección del derecho a la intimidad que asegura la reserva de información sensible o no (estrategia legal, autoincrimina-

ción, noticias) y no bajo el derecho al secreto que protege la reserva del proceso de comunicación a través de vías cerradas facilitadas por terceros. Es decir, solo si se intervinieran teléfonos, cartas, escritos, o, en fin, u otros procesos cerrados facilitados por un tercero, entraría en juego la expectativa razonable de intimidad que tutela el derecho al secreto de las comunicaciones²⁶.

VII. GARANTÍAS PARA LA INVOLABILIDAD DEL SECRETO DE LAS COMUNICACIONES

Ahora debemos poner énfasis en la proclamada intangibilidad del derecho y que se relaciona con la

²⁵ Nótese la importación de ideas. El test de ‘expectativa razonable de privacidad’ fue creado por la jurisprudencia de los Estados Unidos (caso Katz de 1967), aunque no se importó la tutela limitada que otorga esa jurisprudencia a los elementos del proceso de comunicación.

²⁶ De hecho, en España (Sentencia 107/2012), el director de un centro penitenciario accedió a un escrito dirigido por un recluso a un Juez e incluso le inició un proceso sancionador por el contenido del mismo, usando como prueba dicho escrito. El TC español advirtió que se trataba de un agravio contra el secreto de las comunicaciones y no del derecho de la intimidad, pues se había accedido a un proceso comunicativo que pretendía iniciar el recluso con un juez y no con los funcionarios del lugar de reclusión.

doble garantía que prevé el artículo 2.10 de la Constitución: (i) mandato motivado del Juez e; (ii) intervención solo por supuestos previstos en la ley.

A. Mandato previo y motivado de un juez

Esta garantía contiene una reserva de jurisdiccionalidad, pues solo esta autoridad y no un ente administrativo, ni siquiera el legislador, habilitarán la interceptación o apertura de comunicaciones de las personas. La administración podrá colaborar una vez que ya existe la decisión definitiva de un juez en ese asunto y el legislador solo podrá decretar las reglas generales aplicables para que sea legítima dicha intervención.

La decisión del juez será previa a la intervención. La Constitución italiana de 1947 fue la primera en proclamar la exigencia de mandato judicial previo. Allí los miembros de la comisión constituyente italiana –Guia, Conti, Einaudi, Fuschini y Uberti– propusieron la palabra ‘inviolabilidad’ para evidenciar que se imponía una garantía especial frente a la intervención de órganos no judiciales. Aunque coincidían en el argumento, las palabras de Guia fueron las más resaltantes, pues señalaba que:

[...] todos saben lo que sucede con la correspondencia y todos los que han sido juzgados en el período fascista saben que la correspondencia fue controlada, sin que los destinatarios recibieran regularmente las cartas que les habían enviado, por supuesto, después de que la policía había seleccionado las comunicaciones que les interesaba. (2012)

Los comisionados señalaron que sería ingenuo permitir que la policía tenga acceso previo a las comunicaciones, con cargo de dar cuenta a un juez, incluso por razones de seguridad pública. Advirtieron que, si lo interceptado no resulta de interés policial, tampoco tendrán motivo para transmitirlo a la justicia. El carácter oculto de la interceptación genera riesgos que se amplifican si se deja en manos de un solo organismo. Por ello, decidieron que debe ser el juez quien actúe como garante previo, autorizando las intervenciones en las comunicaciones²⁷. En consecuencia, el juez que autorice la intervención tiene la función de proteger el dere-

cho, pero también corre el riesgo de convertirse en su agresor si su decisión incurre en vicios de motivación ausente, aparente, contradictoria o insuficiente (ver por todos, caso Giuliana Llamoya) (Expediente 0728-2008-HC, fundamento 7).

Con motivo de una autorización de escuchas telefónicas, la Corte Suprema argentina señaló que “la exigencia de fundamentación sirve no solo a la publicidad y control republicano, sino que también persigue la exclusión de decisiones irregulares o arbitrarias [...] [pues] pone límite a la libre discrecionalidad del juez, posibilitando el control de sus declaraciones”²⁸ (2013). Por lo tanto, una decisión judicial con vicios de motivación no solo deberá ser invalidada al interior del proceso penal o en un eventual proceso de amparo contra resolución judicial, sino que podrá dar lugar a una eventual responsabilidad por los daños que genere esa errada decisión sobre el sujeto intervenido.

El TEDH advierte que la persona afectada por la interceptación desconoce que el Estado ha ingresado en su esfera de libertad, quedando expuesta. Su única protección será la que establezca el juez, ya que solo de esta manera se evitarán los riesgos de abusos. De ahí la importancia de la intervención judicial y de los límites que el juez debe imponer frente al acceso oculto a los espacios de comunicación cerrada utilizados por los particulares (Kopp, párrafo 64). Por ello, el juez debe verificar que exista un nivel probatorio suficiente para autorizar la intervención. Este requisito lo destaca el TEDH en los casos Roman Zakharov (sentencia del 4 de diciembre de 2015, párrafo 260) y Ekimdzhev (sentencia del 30 de enero de 2008, párrafo 79-80), al señalar que:

[...] [El Juez] debe ser capaz de verificar la existencia de una sospecha razonable contra la persona interesada, en particular, si existen indicios de hecho para sospechar que esa persona planea, comete o haber cometido actos delictivos u otros actos que puedan dar lugar a medidas secretas de vigilancia, como, por ejemplo, actos que pongan en peligro la seguridad nacional. También debe determinar si la interceptación solicitada cumple con el requisito de necesidad en una sociedad democrática [...]

²⁷ La Corte Constitucional italiana entiende que el derecho al secreto de las comunicaciones es “inviolable” en el sentido de que no puede ser objeto de revisión constitucional, ya que incorpora un valor fundacional del sistema democrático deseado por el constituyente. Y agrega que: “... el mismo derecho es inviolable en el sentido de que su contenido de valor no puede ser objeto de restricciones o limitaciones por ninguno de los poderes constituidos, salvo para la realización inderogable de un interés público primario constitucionalmente relevante, siempre que la medida restrictiva sea estrictamente necesaria para la protección de ese interés y se respete la doble garantía de que la normativa prevista responda a los requisitos propios de la reserva absoluta de ley y que la medida restrictiva se disponga mediante un acto motivado de la autoridad judicial” (Corte Constitucional italiana, fundamento tercero del asunto Sentencia 366/1991).

²⁸ Caso Vargas, Registro 2128 y causa 16794, Sentencia del 3 de diciembre de 2013, fundamento III.

incluyendo si es proporcional a los objetivos legítimos perseguidos, verificando, por ejemplo, si es posible lograr los objetivos por medios menos restrictivos²⁹.

Así debe entenderse el artículo 230, incisos 1 y 2, del Nuevo Código Procesal Penal (en adelante, NCPP) cuando dispone que la intervención deberá sustentarse en “suficientes elementos de convicción para considerar la comisión de un delito” y “en mérito a datos objetivos determinados”. En ese sentido la Corte Suprema argentina, en los fundamentos 20 y 21 de la sentencia del 31 de agosto de 2010 (caso Quaranta) nos brinda elementos que debemos considerar al interpretar la norma:

[...] el resultado del hallazgo de un ilícito jamás puede convalidar la falta de motivos objetivos que permitan ex ante fundar una razonable sospecha sobre la perpetración actual de un delito determinado. Otra postura permitiría la intromisión indiscriminada en la vida privada de cualquier persona sin control ni dirección judicial, pues resulta evidente que por cada una de estas ‘expediciones de pesca’ que culminan en el descubrimiento de un delito, muchas otras persecuciones que comprometen los derechos de los ciudadanos permanecen activas y la intimidad de cualquier persona se encuentra expuesta al control y vigilancia constante por parte del estado, todo lo cual resulta decididamente propio de un estado autoritario e incompatible con el goce de los derechos básicos señalados y con la función de un estado de constitucional de derecho³⁰.

En resumen, el objetivo de la persecución y el castigo de los delitos no debe hacernos olvidar que, necesariamente, dentro de ese objetivo, debemos incluir las garantías de respeto a los derechos fundamentales. De lo contrario, estaríamos creando un poder desbocado que pondría en peligro la convivencia social.

B. Mandato previo y motivado de un juez para asuntos no penales

Es posible que un juez decreta la intervención de las comunicaciones en el contexto de procesos disciplinarios o sancionadores, siempre que exista una ley que lo habilite. Por ejemplo, el último párrafo del artículo 60 de la Ley de Carrera Judicial permite que la Oficina de Control de la Magistratura solicite a un juez la adopción de esta medida sobre un investigado. En el caso de Edhin Campos Barrenzuela, la Corte Suprema peruana precisa que tal medida no vulnera, sino que ratifica la reserva jurisdiccional exigida por el derecho a la inviolabilidad de las comunicaciones³¹.

Por lo tanto, la Resolución 237-2021-JNJ, publicada en El Peruano el 8 de abril de 2021, que incorpora el precedente administrativo sobre interceptaciones telefónicas dictado por la Junta Nacional de Justicia (en adelante, JNJ), resulta lesiva para la garantía de jurisdiccionalidad en la intervención de este derecho fundamental. Es decir, el mismo ente que nombra, ratifica y evalúa a jueces y fiscales se convierte en el agente agresor de dicho derecho. En ese precedente se establecen dos criterios:

- (a) La JNJ podrá solicitar al Ministerio Público (en adelante, MP) una copia de las transcripciones de las interceptaciones telefónicas realizadas en el marco de una investigación penal, independientemente de que dichas pruebas aún sean objeto de cuestionamiento judicial. Se presume su validez mientras provengan del MP y no hayan sido invalidadas mediante una resolución judicial firme.
- (b) Si el MP no facilita esa información, la JNJ se auto-faculta para utilizar las transcripciones de las interceptaciones telefónicas realizadas a través de los medios de comunicación, considerándolas como ‘hechos notorios’. En

²⁹ La Corte Suprema argentina sigue una línea similar al invalidar una intervención de las comunicaciones, porque:

[...] el juez no expresó [...] las razones por las cuales consideró procedente la intervención telefónica dispuesta, tampoco remitió a ningún elemento objetivo de la causa que pudiera fundar una mínima sospecha razonable [...] lo único con que se contaba a ese momento consistía, simplemente, en datos aislados y afirmaciones infundadas aportadas por un llamado telefónico anónimo [...] los que resultan manifiestamente insuficientes para brindarle al juez una base sustancial, objetiva, que le permita determinar la existencia de una sospecha razonable, por lo que concluyó que si el Estado pudiera entrometerse en el secreto de las comunicaciones telefónicas a partir de ‘sospechas’ [...] el derecho reconocido constitucionalmente resultaría –ciertamente– de poca o ninguna relevancia. (caso Quaranta, fallos 333:1674, Sentencia del 31 de agosto de 2010, fundamentos 20 y 21)

La Corte Constitucional colombiana (Sentencia C-024/94, fundamento 7.1) recurrió a la jurisprudencia del TEDH y la Corte Suprema de Estados Unidos para resaltar que, en casos como este, el juez debe sustentarse en motivos fundados sobre un conjunto articulado de hechos que permitan inferir de manera objetiva sobre la participación de cierta persona en actos delictivos, de modo que la sospecha o convicción de un agente policial no constituye motivo fundado, ni generan probabilidad y plausibilidad que la persona está vinculada a actividades criminales.

³⁰ Caso Fredes, Registro 2060 y Causa 13.904, Sentencia del 20 de enero de 2013, fundamento III.

³¹ Resolución 6 del 5 de agosto de 2015 (auto de apelación), de la Sala Penal Nacional de la Corte Suprema, Expediente 7-2015 ‘1’.

todo caso, se establece que el administrado podrá exigir al MP que proporcione las transcripciones de las interceptaciones realizadas.

El contenido de este precedente administrativo es alarmante. Desvirtúa por completo la garantía de jurisdiccionalidad del derecho al secreto e inviolabilidad de las comunicaciones. Resulta especialmente preocupante que una entidad denominada ‘Junta de Justicia’ haya olvidado su propia función al establecer criterios de esta naturaleza.

En primer lugar, la Constitución peruana no otorga al MP la facultad de autorizar la intervención en este derecho fundamental. Se establece al juez como garante de este derecho y, por lo tanto, solo él tiene la capacidad de autorizar que otros accedan a la información protegida, como las transcripciones. Además, como se expone, el juez no es un mero tramitador de solicitudes de levantamiento de inmunidad, sino que garantiza que la intervención sea justificada, proporcional y delimitada. De ahí la importancia de su intervención. Sin embargo, sin un fundamento sólido, la JNJ prescinde de su autorización y facultad para requerir al MP que le facilite las transcripciones de las interceptaciones telefónicas, cometiendo una abierta inconstitucionalidad.

En segundo lugar, y de manera aún más grave, la JNJ amenaza con utilizar la información sobre interceptaciones telefónicas que haya sido difundida en los medios de comunicación. Es decir, no solo prescinde del juez, sino también del propio MP. Es inaudito el nivel de desconocimiento de los alcances y garantías del derecho al secreto e inviolabilidad de las comunicaciones. Bastaría que la JNJ revisara el caso Alberto Quimper, en el que el TC peruano precisó la invalidez de tal proceder. Ese caso deja una lección clara: acciones como las que propone la JNJ solo aseguran que se viciará todo el procedimiento y, como consecuencia, que los investigados quedarán exentos de sanción.

Por lo anterior, es preocupante que no se escuchen voces en la academia que cuestionen la propuesta de la JNJ. Más aún cuando el supuesto precedente administrativo vinculante ni siquiera tiene la calidad de norma jurídica (y, por lo tanto, no es susceptible de control jurisdiccional), sino que se trata únicamente de un adelanto de los cri-

terios que la JNJ aplicará en el futuro, lo cual es sumamente lamentable.

C. Calidad de la ley

El sistema jurídico peruano cumple entonces con el dictado de una ley previa que, además, cumple con estándares de claridad o calidad de su contenido. Así, el TC peruano, en el fundamento 363 del caso STC 0003-2005, precisa que debe dictarse una ley que:

[...] de un lado [permita] a los ciudadanos conocer en qué circunstancias y bajo qué condiciones se pueda disponer la intervención o interceptación de comunicaciones; y, de otro, [constituya] un parámetro dentro del cual el juez encuentra delimitada y limitada su competencia discrecional para autorizarla. (fundamento 362)

Es decir, que “regule las garantías que permitan circunscribir el poder discrecional del juez al momento de autorizar la intervención” (Expediente 0003-2005-PI/TC, fundamento 362).

En el mismo fallo, nuestro TC, en los fundamentos 362-364 del Expediente 0003-2005, caso denominado ‘Inconstitucionalidad contra leyes antiterroristas’, aclara que asume los criterios del TEDH sobre las garantías mínimas de la calidad de ley³², como:

[...] la definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial; la naturaleza de las infracciones que puedan dar lugar; la fijación de un límite a la duración de la ejecución de la medidas; las condiciones de tratamiento de los atestados que consignen las conversaciones interceptadas; las precauciones que se deben tomar para comunicar, intactas y completas, las grabaciones realizadas, con el fin de ser controladas eventualmente por el Juez y la defensa; las circunstancias en las que se puede o se debe realizar el borrado o la destrucción de dichas cintas; sobre todo tras un sobreseimiento o una absolución [Caso Valenzuela Contreras c. España, párrafo 46]³³.

Por tanto, en lo que respecta al tiempo, el TC precisa que corresponde al legislador establecer los lí-

³² La exigencia general de ‘calidad de toda ley’ para toda intervención sobre los derechos, puede verse en The Sunday Times, Sentencia del 26 de abril de 1979, párrafo 40.

³³ Un voto del exmagistrado del TC Mesía Ramírez (caso Roberto Nieves) recurre a la jurisprudencia sobre secreto del TEDH en los casos Halford y Copland. Puede ser pertinente señalar que el criterio del caso *Valenzuela contra España* del TEDH (Sentencia del 30 de julio de 1998) que cita nuestro TC, marcó la pauta en otros casos en donde el citado Tribunal analizó la intervención de otros países sobre el mismo derecho, pero el caso *Valenzuela* tuvo la particularidad de que el TEDH condenó a España por no contar con una ley de calidad que regule la intervención en el secreto de comunica-

mites temporales de la intervención. Es decir, la ley debe fijar el plazo máximo de la medida, y el juez deberá motivar adecuadamente por qué eligió un plazo determinado en lugar de uno menor, siempre dentro de los límites temporales establecidos.

A su vez, es esencial establecer criterios que delimiten y justifiquen a los sujetos afectados. Se debe identificar a las personas, sobre las cuales podría recaer la medida, y su relación con los hechos que se pretenden esclarecer. Así, los terceros que no sean investigados ni sospechosos, pero que fortuitamente hayan tenido una comunicación con alguno de ellos, y cuyo tema no esté relacionado con el objeto de la investigación, no podrán ser afectados por la medida de interceptación, por lo que se debe proceder a la destrucción de dichas grabaciones. El TEDH precisa que sería inválido un mandato judicial abierto para intervenir a cualquier persona (sospechosa o no) que pueda tener alguna información sobre el asunto investigado. Además, el tercero afectado debe tener un recurso efectivo que le permita conocer y solicitar la exclusión y destrucción de lo grabado, de acuerdo con el caso Lambert, sentencia del 24 de agosto de 1998, párrafos 38 al 40.

En este sentido, la ley debe precisar las **circunstancias de la intervención**. Su texto debe indicar qué conductas o investigaciones justifican la intervención. El TEDH reconoce que se concede cierta discrecionalidad al juez, pero subraya que esa facultad no puede ser irrestricta, sino que debe estar delimitada por la ley –caso Silver en el párrafo 88–. Por ejemplo, debe especificarse la naturaleza o tipología de los ilícitos que pueden habilitar las intervenciones. En los casos Valenzuela, Prado Bugallo, Kruslin (Sentencia del 24 de abril de 1990) y Huving (Sentencia del 24 de abril de 1990), el TEDH invalidó las regulaciones que permitían la interceptación solo para esclarecer hechos vinculados a un proceso penal. En el caso Malone, consideró ilegítimas las leyes que habilitaban in-

tervenciones, en general, para determinar la ocurrencia de delitos, y en el caso Liberty consideró lesivas las leyes que no fijaban parámetros materiales para la intervención, sino que las habilitaban para todo tipo de comunicación que llegara a un país con la mera invocación de proteger la ‘seguridad nacional’, la ‘detección de delitos graves’ o el ‘bienestar económico’³⁴. Y es que, como se señala en el caso Roman Zakharov (Sentencia del 4 de diciembre de 2015), se debe identificar claramente la naturaleza de los delitos que justificarían una orden de interceptación, así como las personas a las que alcanzaría.

Lo anterior está relacionado con la razonabilidad de la intervención, pues como señala el TC español en el fundamento 4 del caso Sentencia 167/2002, esta solo será legítima si es:

[...] necesaria para alcanzar un fin constitucionalmente legítimo, como, entre otros, para la defensa del orden y prevención de delitos calificables de infracciones punibles graves y es idónea e imprescindible para la investigación de los mismos [...]. [Sentencia 166/1999, de 27 de septiembre, FJ 3 a] (TC de España, 2002)

Por tanto, sería ilegítima, por ser poco previsible y desproporcionada, cualquier regulación que pretenda intervenir en el secreto de las comunicaciones para investigar todo tipo de delitos, sin una identificación precisa de cuáles delitos graves justificarían tal medida.

Por último, debe preverse **un control ex post** para la recolección, supervisión y eventual eliminación de la información intervenida. El TEDH exige que la ley tome ciertas precauciones al respecto. En el caso Kopp se cuestionó la falta de regulación sobre la supervisión judicial de los funcionarios administrativos que accedían a los datos; y en el caso Liberty, se criticó la existencia de una regulación que habilitara la interceptación de todas las

ciones. Y es que su ley procesal penal no indicaba de manera suficiente en qué circunstancias y bajo qué condiciones el juez podría realizar tales intervenciones. A pesar de que se modificó esa regulación, en el caso Prado Bugallo se consideró insuficiente el nuevo régimen español, pues no se garantizaba que las comunicaciones estén intactas y completas para su control eventual por el juez y la defensa. España siguió sin modificar su legislación, y solo su TC estableció parámetros de intervención, por lo que volvió a ser condenada en el caso Abdulkadir Coban (Sentencia del 26 de septiembre de 2006). Ver también el caso Prado Bugallo (Sentencia del 18 de febrero de 2003). Para ventura de sus ciudadanos, los criterios del TEDH han sido desarrollados y aplicados por el TC español (Sentencia 49/1999 y Sentencia 184/2003).

³⁴ En Argentina, la Corte Suprema estimó inconstitucional la Ley 25.873 que disponía que, ante el requerimiento del Poder Judicial o del MP, las empresas concesionarias debían permitirles el acceso remoto a las comunicaciones de los usuarios. Esa Corte recurrió a la jurisprudencia del TEDH y del TC español para concluir que:

[...] sus previsiones [legales] no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones [...] tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales [...] resulta inadmisibles que las restricciones autorizadas por la ley estén desprovistas del imprescindible grado de determinación que excluya la posibilidad de que su ejecución concreta por agentes de la Administración quede en manos de la más libre discreción de estos últimos. (caso Halabi, fallos 332:111, Sentencia del 24 de febrero de 2009, fundamento 26)

comunicaciones comerciales submarinas que llegaban a un país, sin especificaciones adicionales, e incluso la ausencia de normas publicadas para la selección, examen, uso, conservación y destrucción de esos datos. En el caso Valenzuela, Prado Bugallo, Kruslin y Huving se consideró ilegítima la falta de medidas para conservar la información recabada, de manera que tanto el juez como el afectado pudieran revisarla, controlarla y ejercer la defensa, respectivamente. Incluso se señaló la falta de regulación que asegurara la reserva y destrucción de los datos cuando la causa sea sobreseída o el procesado absuelto.

De cualquier modo, la eventual insuficiencia legislativa no justifica vulnerar el derecho al secreto de las comunicaciones, ya que los jueces pueden ser tanto garantes como agresores de este derecho al dictar mandatos genéricos de intervención, sin precisar el objeto de la investigación ni la información perseguida de acuerdo con el caso Van Rossem, Sentencia del 9 de marzo de 2005, párrafos 44 al 51.

VIII. CONCLUSIONES

Este trabajo de integración comparada ha generado los siguientes criterios y principios que deben regir el derecho al secreto e inviolabilidad de las comunicaciones:

- Su objeto protege el secreto de un proceso de comunicación y abarca todos sus elementos, incluyendo la comunicación recibida y archivada, ya que su propósito no es solo el secreto de lo comunicado, sino también el secreto sobre la existencia misma de dicho proceso.
- Tiene un contenido formal, ya que protege el proceso de comunicación, independientemente de la trascendencia, sensibilidad, intimidad o irrelevancia de lo comunicado.
- Por ello, se ejerce cuando se utilizan canales cerrados de comunicación o aquellos en los que se puede esperar razonablemente el secreto del proceso comunicativo.
- Esos canales cerrados deben ser administrados o facilitados por terceros que garanticen el secreto del proceso comunicativo, protegiéndolo frente a los riesgos de ‘apertura’, ‘incautación’, ‘interceptación’ o ‘intervención’ por parte de sujetos ajenos al proceso.
- Es un derecho que forma parte de los espacios protegidos por la concepción formal de la intimidad, pero está sujeto a un régimen jurídico diferenciado que busca mantener en

un ámbito reservado la existencia misma de los procesos de comunicación.

- En este sentido, el derecho al secreto e inviolabilidad de las comunicaciones procura, al igual que la intimidad, la protección de aquellos espacios en los que existe una ‘expectativa razonable de privacidad’.
- Cuenta con garantías distintas a las de la intimidad, ya que su intervención solo es posible mediante un mandato motivado por el juez y con las garantías establecidas por la ley, mientras que para intervenir el derecho a la intimidad basta con una adecuada ponderación con otros derechos o fines valiosos.
- La garantía del mandato judicial busca hacer proporcional la intervención oculta sobre la libertad de las comunicaciones, por lo que debe activarse únicamente en casos de especial gravedad y cuando existan elementos objetivos que justifiquen su necesidad.
- La garantía de ley exige que la regulación identifique claramente los supuestos de interceptación, los sujetos involucrados, el tiempo de intervención, así como las garantías para el acceso, manejo, fiscalización y destrucción de la información, muchas de las cuales no son respetadas por nuestra legislación.

A pesar de que la intervención en las comunicaciones desempeña un papel crucial en los casos judiciales más notorios de nuestro país, la comprensión de sus alcances sigue siendo poco clara. Por tanto, existe el riesgo de que vicios y errores desacrediten las investigaciones, lo que podría resultar en la violación de las garantías constitucionales y, en consecuencia, en la anulación de procesos penales que realmente perseguían hechos delictivos. Esta es la trascendencia del asunto. ¶

CONFLICTO DE INTERESES

El autor declara expresamente que no existen conflictos de intereses que hayan influido en la elaboración, evaluación ni publicación del presente artículo.

FUENTES DE FINANCIACIÓN

El autor declara que no han recibido financiamiento externo para la realización de la presente investigación.

ESTÁNDARES ÉTICOS

El autor manifiesta que esta investigación ha sido desarrollada conforme con los principios y estándares éticos aplicables a la labor académica e investigativa.

REFERENCIAS

- Alcaraz, H. (2004). Jurisprudence du Conseil constitutionnel. 1er juillet - 30 septembre 2004. *Revue française de droit constitutionnel*, (60), 797-831.
- Amsterdam, A. (1974). Perspectives on the Fourth Amendment. *Minnesota Law Review*, 58(3), 349-477.
- Armand, G. (2006). Que reste-t-il de la protection constitutionnelle de la liberté individuelle? *Revue française de droit constitutionnel*, (65), 37-72.
- Boix Reig, J. (Dir.) & Jareño Leal, Á. (Coord.). (2010). *La protección jurídica de la intimidad*. Iustel.
- Diggelmann, O. & Cleis, M. (2014). How the right to privacy became a human right. *Human Rights Law Review*, 14(3), 441-458.
- Epping, V. (2019). *Grundrechte*. Springer.
- Freiwald, S. & Smith, S. (2018). The Carpenter Chronicle: A near-perfect surveillance. *Harvard Law Review*, 132(1), 205-235.
- Galli, F. (2016). The interception of communication in France and Italy—what relevance for the development of English law? *The International Journal of Human Rights*, 20(5), 666-683.
- Gargarella, R. & Guidi, S. (2016). *Comentarios de la Constitución de la Nación Argentina. Jurisprudencia y doctrina: una mirada igualitaria* (Tomo I). La Ley.
- Gelli, M. (2018). *Constitución de la Nación Argentina: comentada y concordada* (Tomo I). La Ley.
- Gusy, C. (2011). *Grundrechte und Verfassungsschutz*. Springer.
- (2018). Art. 10. En M. Mangoldt, F. Klein, & H. Starck (Eds.), *Kommentar zum Grundgesetz* (7a ed., tomo I). C. H. Beck.
- Halpérin, J. (2005). L'essor de la «privacy» et l'usage des concepts juridiques. *Droit et société*, (61), 765-782.
- Halpérin, J. (2015). Protection de la vie privée et privacy: deux traditions juridiques différentes? *Les nouveaux cahiers du conseil constitutionnel*, (48), 59-68.
- Harris, D., O'boyle, M., Bates, E. & Buckley, C. (2018). *Harris, O'Boyle, and Warbrick: Law of the European Convention on Human Rights* (5a ed.). Oxford University Press.
- Jareño, Á. (2008). *Intimidad e imagen: los límites de la protección penal*. Iustel.
- Janis, M., Kay, R., & Bradley, A. (2000). *European Human Rights Law: Text and Materials*. Oxford University Press.
- Lasagabaster, I. (Dir.). (2009). *Convenio europeo de derechos humanos: comentario sistemático* (2a ed.). Editorial Civitas.
- López, H. (2000). Hacia un concepto formal del derecho a la intimidad y sus consecuencias. *Repertorio Aranzadi del Tribunal Constitucional*, (2), 1885-1898.
- Martín, R. (1995). *El régimen constitucional del secreto de las comunicaciones*. Editorial Civitas.
- Medina, M. (2005). *La protección constitucional de la intimidad frente a los medios de comunicación*. Tirant lo Blanch.
- Moreham, N. (2008). The right to respect for private life in the European Convention on Human Rights: A re-examination. *European Human Rights Law Review*, (1), 44-79.
- Mowbray, A. (2005). The development of positive obligations under the European Convention on Human Rights by the European Court of Human Rights. *Human Rights Law Review*, 5(1), 191-195.
- Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 57, 1701-1777.
- Pace, A. (1985). *Problematica delle libertà costituzionali*. Padua: CEDAM.
- Pagenkopf, M. (2021). Art. 10. En M. Sachs (Ed.), *Grundgesetz - Kommentar* (9a ed.). C. H. Beck.
- Peyrat-Guillard, D. (2012). Le respect de la vie privée des salariés. Quels enjeux pour les entreprises et les organisations syndicales? *Revue française de gestion*, (224), 153-172.
- Rebollo, L. (2005). *El Derecho fundamental a la intimidad*. Dykinson.
- Ribes, D. (2015). Atteintes publiques et atteintes privées au droit au respect de la vie privée

dans la jurisprudence du Conseil constitutionnel. *Les Nouveaux Cahiers du Conseil constitutionnel*, (48), 35-46.

Ridaura, M. (2017). El legislador ausente del artículo 18.3 de la Constitución (la construcción pretoriana del derecho al secreto de las comunicaciones). *Revista de Derecho Político*, (100), 347-404.

Rivero, F. (2017). *Revisión del concepto constitucional del secreto de las comunicaciones*. Dykinson.

Rodríguez, J. (2011). Sobre la naturaleza formal del derecho al secreto de las comunicaciones: dimensión constitucional e histórica. *Diario La Ley*, Nº 7647, Sección Doctrina, 8 de junio de 2011.

Rozenshtein, A. (2019). Fourth Amendment Reasonableness after Carpenter. *Yale Law Journal Forum*, (128), 943-960.

Sachs, M. (2017). *Verfassungsrecht II – Grundrechte*. Springer.

Schabas, W. (2015). *The European Convention on Human Rights: A commentary*. Oxford University Press.

Sosa, J. (2018). La libertad constitucional. Tres modelos esenciales de libertad y tres derechos de libertad. *Pensamiento Constitucional*, 23(23), 177-203.

Steiner, C. & Uribe, P. (Eds.). (2014). *Convención Americana sobre Derechos Humanos. Comentarios*. Fundación Konrad Adenauer Stiftung.

Talitz, A. (2006). *Reconstructing the Fourth Amendment: A history of search and seizure, 1789-1868*. New York University Press.

Tamò-Larrieux, A. (2018). *Designing for Privacy and its Legal Framework*. Springer.

Van Dijk, P., Van Hoof, F., Van Rijn, A. & Zwaak, L. (2006). *Theory and practice of the European Convention on Human Rights*. Intersentia.

Velásquez, R. (2010). Delimitación del derecho fundamental al secreto e inviolabilidad de las comunicaciones. En J. M. Sosa Sacio (Coord.), *Los derechos fundamentales* (pp. 193-228). Gaceta Jurídica.

Warren, S. & Brandeis, L. (1995). *El derecho a la intimidad* (introducido por Benigno Pendás y traducido por Pilar Baselga). Editorial Civitas.

Winn, P. (2016). Katz and the origins of the reasonable expectation of privacy test. *McGeorge Law Review*, 40(1), 1-12.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Bundesverfassungsgericht, 14 de julio de 1999, Sentencia BVerfGE 85, 386 (Alemania).

Bundesverfassungsgericht, 2 de marzo de 2004, Sentencia BVerfGE 106, 28 (Alemania).

Bundesverfassungsgericht, 15 de diciembre de 2006, Sentencia BVerfGE 115, 166 (Alemania).

Constitución Política del Perú [Const.] (1993).

Corte Constitucional, 21 de noviembre de 1996, Sentencia C-626/96 (Colombia).

Corte Costituzionale, 11 de julio de 1991, Sentencia 366/1991 (Italia).

Corte Costituzionale, 26 de febrero de 1993, Sentencia 81/1993 (Italia).

Corte Interamericana de Derechos Humanos. *Caso Fontevecchia y D'Amico c. Argentina*, 29 de noviembre de 2011.

Corte Interamericana de Derechos Humanos. *Caso Vargas* (Registro 2128, causa 16794), 3 de diciembre de 2013.

Cour de Cassation, 2 de octubre de 2001, Caso Nikon (Francia).

Supreme Court of the United States, 5 de marzo de 1877, Ex parte Jackson (Estados Unidos).

Supreme Court of the United States, 18 de diciembre de 1967, Katz c. United States (Estados Unidos).

Supreme Court of the United States, 20 de junio de 1979, Smith c. Maryland (Estados Unidos).

Tribunal Constitucional [T.C.], 14 de julio de 2002, sentencia recaída en el Expediente 00943-2016-PA/TC (Perú).

Tribunal Constitucional [T.C.], 29 de enero de 2003, sentencia recaída en el Expediente 2863-2002-AA/TC (Perú).

Tribunal Constitucional [T.C.], 20 de setiembre de 2004, sentencia recaída en el Expediente 0134-2003-HD/TC (Perú).

Tribunal Constitucional [T.C.], 8 de marzo de 2005, sentencia recaída en el Expediente 0774-2005-HC/TC (Perú).

Tribunal Constitucional [T.C.], 22 de noviembre de 2005, sentencia recaída en el Expediente 7811-2005-PA/TC (Perú).

Tribunal Constitucional [T.C.], 9 de agosto de 2006, sentencia recaída en el Expediente 003-2005-PI/TC (Perú).

Tribunal Constitucional [T.C.], 28 de setiembre de 2009, sentencia recaída en el Expediente 3901-2007-PA/TC (Perú).

Tribunal Constitucional [T.C.], 27 de octubre de 2010, sentencia recaída en el Expediente 00655-2010-PHC/TC (Perú).

Tribunal Constitucional [T.C.], 19 de julio de 2011, sentencia recaída en el Expediente 04224-2009-PA/TC (Perú).

Tribunal Constitucional [T.C.], 17 de julio de 2014, sentencia recaída en el Expediente 00867-2011-PA/TC (Perú).

Tribunal Constitucional [T.C.], 10 de marzo de 2016, sentencia recaída en el Expediente 03485-2012-PA/TC (Perú).

Tribunal Constitucional [T.C.], 22 de febrero de 2017, sentencia recaída en el Expediente 05532-2014-PA/TC (Perú).

Tribunal Constitucional, 29 de noviembre de 1984, Sentencia 114/1984 (España).

Tribunal Constitucional, 11 de marzo de 1996, Sentencia 34/1996 (España).

Tribunal Constitucional, 22 de julio de 1999, Sentencia 144/1999 (España).

Tribunal Constitucional, 3 de abril de 2002, Sentencia 70/2002 (España).

Tribunal Constitucional, 20 de mayo de 2002, Sentencia 123/2002 (España).

Tribunal Constitucional, 18 de septiembre de 2002, Sentencia 167/2002 (España).

Tribunal Constitucional, 30 de junio de 2003, Sentencia 127/2003 (España).

Tribunal Constitucional, 27 de marzo de 2006, Sentencia 89/2006 (España).

Tribunal Constitucional, 5 de noviembre de 2007, Sentencia 230/2007 (España).

Tribunal Constitucional, 7 de noviembre de 2011, Sentencia 173/2011 (España).

Tribunal Constitucional, 2 de julio de 2012, Sentencia 142/2012 (España).

Tribunal Europeo de Derechos Humanos. *Caso Halford c. Reino Unido*, 25 de junio de 1997.

Tribunal Europeo de Derechos Humanos. *Caso Amann c. Suiza*, 16 de febrero de 2000.

Tribunal Europeo de Derechos Humanos. *Caso Von Hannover c. Alemania*, 24 de junio de 2004.

Tribunal Europeo de Derechos Humanos. *Caso Copland c. Reino Unido*, 3 de abril de 2007.

Tribunal Europeo de Derechos Humanos. *Caso Asociación para la Integración Europea y los Derechos Humanos y Ekimdzhiev c. Bulgaria*, 30 de enero de 2008.

Tribunal Europeo de Derechos Humanos. *Caso Roman Zakharov c. Rusia*, 4 de diciembre de 2015.