IMPLEMENTACIÓN DE LA IDENTIFICACIÓN DE USUARIOS, TERMINALES O DISPOSITIVOS DE CONECTIVIDAD SIN AUTORIZACIÓN JUDICIAL EN LA NORMATIVA PERUANA

M5.258 - Trabajo Final de Máster

Juan Carlos Jara Luna
Máster Universitario en Ciberdelincuencia

Tutor: Dr. Alberto Varona Jiménez

Piura, junio del 2022

Índice

Introducción

El auge de las tecnologías de la información y comunicación [TIC], como elemento para facilitar el intercambio de información de diversa índole, y su facilidad para favorecer el dinamismo económico, ha supuesto un cambio sobre la delincuencia tradicional, denotando realce en sentido cuantitativo, debido al desarrollo que ha tenido el uso de internet, llegando cada día a más lugares; y en sentido cualitativo, esa misma expansión ha permitido que a la par se gesten nuevas formas de criminalidad, las cuales han sido denominadas como “cibercrimen”. Este término abarca todas las tipologías de comportamientos que tienen como común denominador la comisión de la conducta delictiva a través de las TIC e Internet (Miró, 2012).

En la República del Perú, para la lucha contra este tipo de fenómeno tenemos la Ley N° 30096 - Ley de Delitos Informáticos -publicada el 22 de octubre del 2013 y modificada mediante la Ley N° 30171 del 10 de marzo del 2014. Asimismo, en el año 2019, nos pusimos en sintonía con otros ordenamientos y suscribimos el Convenio sobre la Ciberdelincuencia adoptado el 23 de noviembre del 2001 en la ciudad de Budapest, el cual fue aprobado mediante Resolución Legislativa N° 30913 el 13 de febrero del 2019, entrando en vigor el 01 de diciembre del 2019.

Ya operativamente, el 30 de diciembre del 2020, se creó la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional, la cual tiene entre sus funciones la de orientación, coordinación y unificación de criterios con las fiscalías a nivel nacional, brindando acompañamiento técnico a estas (El Peruano, 2020) y, recién en el año 2021, se ha creado una fiscalía especializada en ciberdelincuencia pero concentrada en la capital del país, no habiendo extendido este acertado criterio a provincias (El Peruano, 2021).

Como es de esperarse, debido a nuestra reciente apertura hacia este paradigma y, por tanto, estudio de este fenómeno, hay muchas falencias al momento de abordar esta realidad desde perspectivas tanto criminológicas, victimológicas, penales y procesales.

Bajo este contexto, desde mi perspectiva como parte integrante del sistema de administración de justicia -teniendo mi país un sistema procesal penal principalmente acusatorio- al desempeñarme como asistente en función fiscal en el Ministerio Público – Fiscalía de la Nación, he podido percibir a prima facie que, a pesar de la legislación especializada que el parlamento ha proveído sobre la materia, aún estamos lejos del nivel que tienen ordenamientos jurídicos como el español, que han cubierto en gran medida -con legislación y jurisprudencia- aquellos eslabones tan esenciales que a veces suelen pasar inadvertidos, y que en nuestro caso, por nuestra propia inexperiencia, hemos pasado por alto.

Por lo expuesto, este trabajo de investigación busca desde la legislación comparada, postular ciertas reformas -o un mejor abordaje- desde la perspectiva del derecho penal adjetivo, y brindar a los operadores de justicia las herramientas necesarias para abordar de manera adecuada este nuevo paradigma y suplir aquellos aspectos problemáticos que se han ubicado, principalmente, en cuanto a la celeridad de las investigaciones fiscales al abordar la ciberdelincuencia. Ello, atendiendo a la gran carga procesal generada por estos casos en los últimos años, y a su vez, al deficiente resultado que se ha obtenido producto de la investigación fiscal, lo cual ha dado como resultado una marcada sensación de inseguridad e impunidad (OFAEC, 2021).

Delimitación del Tema de Investigación

La presente investigación, por sus propias características, no pretende explorar las diferentes normativas procesales de los ordenamientos jurídicos más desarrollados en búsqueda de las mejores medidas de investigación tecnológica, sino que tendrá como único punto de referencia la normativa española, la cual -a mi consideración- ha estructurado y desarrollado adecuadamente estas. En este sentido, tampoco se pretende ser extensivos y profundizar en todos los recursos que prevé el régimen jurídico-procesal español, los cuales están contemplados en los capítulos IV, V, VI, VII, VIII, IX y X del título VIII, libro II de la Ley de

Enjuiciamiento Criminal; ya que un análisis de esta naturaleza requeriría una mayor expansión y recursos en cuanto a tiempo y dedicación.

Por lo tanto, se ha elegido un punto neurálgico y a la vez práctico para iniciar con esta apertura a una nueva perspectiva sobre el abordaje de la investigación tecnológica en la ciberdelincuencia. Es así, que éste trabajo se centrará en las medidas tecnológicas que no requieren autorización judicial, específicamente la contenida en el artículo 588 ter m de la Ley de Enjuiciamiento Criminal, referida a la identificación de titulares o terminales o dispositivos de conectividad, la cual señala lo siguiente:

> Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia.

Siendo este artículo, parte de la reforma de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015, del 5 de octubre.

Si bien este artículo, como se ha podido percibir, es sólo una de las herramientas frente a todas las posibilidades procesales que pueden emplearse en una investigación en materia de ciberdelincuencia. Se eligió, debido a que la normativa procesal peruana, sobre este punto, no ha previsto bajo ninguna circunstancia, la posibilidad de que el Ministerio Público requiera directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, que brinden directamente -sin mediar un requerimiento a través del órgano jurisdiccional- la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o,

en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación.

Planteamiento del Problema

El principal problema radica en que la legislación peruana, no cuenta con un mecanismo procesal adecuado para obtener información primaria y directa de los proveedores de servicios de comunicación sobre la identidad de sus usuarios.

Esto es un aspecto muy relevante, ya que, usualmente, cuando se empieza una investigación por una estafa, ciberacoso, ciberfraude o suplantación de identidad -por citar solo algunos ejemplos-, no se cuenta con mayores datos de identificación mas que un número celular o un nombre de usuario. Siendo, por tanto, actualmente necesario requerir a un juez de garantías para que proceda con el levantamiento del secreto de las comunicaciones, con la finalidad de autorizar a que la empresa prestadora del servicio otorgue, al menos, los datos de identidad del investigado. Circunstancia que, debido a la gran carga procesal que tienen estos juzgados, ralentiza el proceso de investigación -el cual preliminarmente tiene como máximo120 días- dilatándolo excesivamente ya que en los casos mencionados puede durar meses, incluso más de un año, hasta que el jugado atienda el requerimiento, sin perjuicio del tiempo que se demore la empresa en proveer la información.

Si bien la normativa peruana ha previsto mediante su Código Procesal Penal y a través de sus órganos encargados, en este último caso el Organismo Supervisor de la Inversión Privada en Telecomunicaciones, ciertas normativas –como la Resolución de Consejo Directivo Nº 107-2016-CD-OSIPTEL- donde se obliga a las empresas de servicios públicos de telecomunicaciones a colaborar de manera célere con los requerimientos de información realizados por los órganos jurisdiccionales bajo sanción de multa. Estas medidas, no han hecho eco dentro de los procedimientos realizados por los operadores de justicia, ya que siguen existiendo notables limitaciones en cuanto a la pronta atención de estas solicitudes.

Como se puede apreciar, este aspecto es perjudicial, ya que la información más relevante que es la identidad del posible autor del hecho, identificación del equipo o del dispositivo de conectividad correspondiente, llega muchos meses después de iniciada la investigación, lo cual evita que se realicen diligencias urgentes e inmediatas para determinar la responsabilidad penal del agente y sobre todo para evitar que la prueba digital pueda perderse.

Por lo tanto, el procedimiento hasta ahora estandarizado resultaría tedioso e infructuoso, pues dentro de una investigación -como se expresó en los párrafos anteriores- se tiene la necesidad de solicitar al juez de garantías la emisión de una resolución para autorizar a las empresas de telefonía a brindar información sobre la identidad del titular del servicio. Sin embargo, irónicamente, cualquier persona con tan solo su documento nacional de identidad puede ingresar, por ejemplo, al aplicativo móvil Yape o Plin -empleados en comercios menores o transacciones de montos bajos, para el envío y recepción de dinero- y digitar el número telefónico de una persona y obtener datos sobre su identidad. Siendo esto último beneficioso para una investigación, ya que podría ser utilizado -en cierto modo- como datos de fuente abierta o, por el contrario, con el empleo de ingeniería social resultar perjudicial y conllevar a que la persona sea una potencial víctima de algún ciberdelito.

La situación antes descrita, se contrasta con la realidad que provee la legislación española, la cual cuenta con una normativa específica en su Ley de Enjuiciamiento Criminal, concretamente el precepto contenido en el Artículo 588 ter m, relacionados al acceso a datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, sin que sea necesario que se dicte una autorización judicial cuando se requieran en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet.

En este punto, es necesario precisar que, esto no fue siempre un criterio estandarizado por el legislador español, pues antes de la reforma operada por la Ley Orgánica 13/2015, del 5 de octubre, existían criterios doctrinarios diferentes y normativa -cómo la Ley 25/2007, de 18 de octubre- que exigían una autorización

judicial para obtener mínimamente los datos tratados por las empresas de telefonía para identificar al usuario o titular de un número en específico; siendo la situación antes descrita, símil a la situación actual que enfrenta el sistema procesal peruano.

Por lo tanto, ante el problema planteado, desde la evaluación comparada se pretende dar respuestas las siguientes preguntas problematizadoras:

Pregunta Principal:

1. ¿Es viable implementar las medidas de investigación sin autorización judicial de la legislación española, referentes al acceso a datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, a la legislación peruana?

Preguntas Secundarias:

1. ¿La legislación peruana, atendiendo a su normativa interna, podría prescindir del levantamiento judicial del secreto de las comunicaciones para obtener la identificación de usuarios, terminales y dispositivos de conectividad?
2. ¿Se vulnera el derecho a la intimidad, el secreto de las comunicaciones o la Ley de Protección de Datos Personales peruana, si se autoriza a las empresas proveedoras de servicios de comunicación a brindar los datos de identificación de usuarios, terminales y dispositivos de conectividad, sin que sea necesario una orden judicial para dicho fin?

Justificación

La justificación de esta investigación tiene dos parámetros a destacar. El primero, es explorar y comprender las razones que motivaron al legislador español a llevar a cabo las reformas del 2015, que modificaron la Ley de Enjuiciamiento Criminal y tuvieron por finalidad fortalecer las garantías procesales y la regulación de las medidas de investigación tecnológica. Específicamente, este trabajo se

centrará en los fundamentos empleados para la introducción del artículo 588 ter m, referido a la identificación de titulares o terminales o dispositivos de conectividad.

La medida objeto de evaluación, como ya se mencionó, forma parte de aquellas que no requieren del presupuesto de jurisdiccionalidad para ejecutarse, según se refiere, al no afectar el secreto a las comunicaciones, tener una incidencia mínima en el derecho a la intimidad y no excederse en las exigencias de la Ley de protección de datos (Iberley, 2019). En este sentido, bajo estas últimas premisas, se pretende hacer un análisis comparado donde se evalúe si estos criterios pueden ser replicados y asumidos por el sistema procesal penal peruano, atendiendo a su configuración actual y la normativa que lo rige.

El segundo parámetro, está relacionado al logro académico que se pretende por esta investigación, ya que este análisis, de ser favorable, permitirá que se postule una reforma normativa o un nuevo enfoque de criterios que beneficie a los operadores de justicia en la obtención célere de información sobre los datos de identificación de usuarios, terminales y dispositivos de conectividad. Esto, tendrá un efecto trascendental en el abordaje de la ciberdelincuencia, específicamente en la duración de las investigaciones, facilidad en la obtención de elementos de convicción y, sobre todo, en aliviar la sensación de inseguridad e impunidad (OFAEC, 2021).

Asimismo, se pretende proyectar nuevos criterios en cuanto a la apertura del sistema procesal peruano al nuevo paradigma de la ciberdelincuencia, donde -a mi consideración- es necesario actualizar algunos criterios que se han quedado estancados a lo largo de los años, y que no se condicen con la finalidad del proceso penal, específicamente la represiva. La cual, bajo la luz de un modelo acusatorio garantista, insta a que la labor de los operadores de justicia esté sujeta a diversos principios y garantías que orienten su desarrollo, con la finalidad de que se ejecute conforme a la constitución y en aras de un debido proceso (Reátegui, 2008, pág. 92); pero, como efecto adverso, hace que -en muchos casos- se haga erróneamente

una interpretación extensiva de ciertos derechos, perjudicando las investigaciones cuando se ven involucradas las TIC.

Teniendo en cuenta estas consideraciones, sería un buen punto de partida, a partir de la confrontación entre los sistemas jurídicos peruano y español – en cuanto al abordaje del cibercrimen, para plantear en el futuro nuevas reformas normativas al sistema jurídico de Perú, evaluando los procedimientos en la materia específica, sus efectos procesales y su sustento normativo. De esta manera, se podría contribuir en el acervo doctrinario desde la óptica de la ciberdelincuencia, en un mejor abordaje de delitos como el fraude informático, los relativos a la propiedad intelectual, a la intimidad, entre otros; así como proponer medidas de prevención e intervención de la cibervictimización en todas sus variantes, ya sea social, económica o política (Agustina et all, 2020).

Contenido y límites

Para finalizar la introducción, es necesario precisar que, este trabajo está estructurado para desarrollar de manera ordenada y sistemática, todos los aspectos relevantes que permitan dar una posible solución al problema planteado. Para este fin, en los apartados siguientes, se pretende realizar un análisis comparado de la jurisprudencia, doctrina y legislación tanto española como peruana, bajo una metodología jurídico-comparada. Esto permitirá dar respuesta a las preguntas problematizadoras planteadas, validar nuestra hipótesis y exponer nuestras conclusiones, en aras de una mejora en la investigación de cibercrímenes de manera célere y eficaz.

Estado de la Cuestión

Como se señaló en la parte introductoria, en la República de Perú, el nuevo paradigma de la ciberdelincuencia es una realidad que en estos últimos años ha tomado especial importancia, a razón de la pandemia SARS-COV2-COVD 19 y las nuevas tecnologías que han ido surgiendo en el mercado, desde la expansión de redes de comunicación mucho más rápidas a todos los rincones del país (OSIPTEL,

2022), hasta el uso cotidiano de nuevos aplicativos móviles para dinamizar las relaciones interpersonales y transacciones económicas. Esto ha generado, en palabras de Fernando Miró (2011, pág. 17), un ámbito distinto de oportunidad delictiva, que genera un riesgo criminal diferente al espacio físico tradicional.

Sin embargo, si bien desde el año 2013 Perú cuenta con una ley específica para abordar este tipo de criminalidad - Ley N° 30096 - Ley de Delitos Informáticos, no es hasta el año 2019, con la suscripción del Convenio sobre la Ciberdelincuencia, que se ha prestado un mayor interés a este fenómeno, siendo a partir de este momento que se crean fiscalías especializadas como la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional, asociaciones civiles orientadas a la investigación de la ciberdelincuencia como lo es el Observatorio Peruano de Cibercriminalidad, aunado al visible incremento de capacitaciones sobre la materia. Pese a ello, el desarrollo doctrinario que se ha dado resulta escaso, limitándose principalmente al desarrollo de la Ley de Delitos Informáticos, a los tipos penales que la integran, las falencias en cuando al abordaje de estos y ciertos riesgos relacionados con la cibervictimización económica y social.

Como se puede apreciar, no se ha logrado ubicar antecedentes que sigan nuestro planteamiento, esto es, trabajos de investigación que evalúen desde una óptica comparada, aquellos aspectos procesales que limitan la actuación de los operadores de justicia para la investigación de delitos cometidos a través de las TIC e internet. Bajo este contexto, es que se puede afirmar que la presente investigación es original, y que, más allá de sistematizar información bibliográfica, parte del análisis de las limitaciones observadas desde mi panorama laboral, en el ámbito del desarrollo de procedimientos de investigación fiscal.

Diseño Metodológico

Hipótesis

Con base a las preguntas que sostiene la problemática expuesta, las hipótesis propuestas son las siguientes:

Hipótesis Principal

1. Es viable implementar las medidas de investigación sin autorización judicial de la legislación española, referentes al acceso a datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, a la legislación peruana

Hipótesis Secundarias

1. No hay impedimento normativo en la legislación peruana para poder prescindir del levantamiento judicial del secreto de las comunicaciones y obtener directamente la identificación de usuarios, terminales y dispositivos de conectividad.
2. No se vulnera el derecho a la intimidad, al secreto de las comunicaciones o a Ley de Protección de Datos Personales peruana, si se autoriza a las empresas proveedoras de servicios de comunicación a brindar sin autorización judicial, los datos de identificación de usuarios, terminales y dispositivos de conectividad, ya que al solo brindar la identificación y no abordar el tráfico de la comunicación, no se trastoca ninguna de estas esferas.

Tipo de Investigación

Para poder comprobar nuestras hipótesis, se ha visto conveniente desarrollar una investigación de tipo documental, mediante la cual, a través de una técnica cualitativa, se recopilará y seleccionará información de los dos ordenamientos jurídicos escogidos, que son el peruano y el español.

Método de investigación

Se ha considerado como método más adecuado para abordar el tema propuesto a la metodología jurídico-comparada, la cual nos permitirá dilucidar la viabilidad de implementar a la legislación peruana, la normativa española referente a las medidas de investigación sin autorización judicial, referentes al acceso a datos

necesarios para la identificación de usuarios, terminales y dispositivos de conectividad.

En este sentido, siguiendo la propuesta de Marchal (2017, pág. 51-53) respeto a la adecuada investigación bajo la metodología comparada, para poder corroborar nuestras hipótesis, se realizará un estudio del sistema jurídico español y peruano, ahondando en cómo se ha resuelto o intentado resolver en cada país la problemática planteada, para ello se analizarán fuentes normativas, instituciones, doctrina y/o jurisprudencia, que permitan estudiar las equivalencias o divergencias entre los regímenes jurídicos y encontrar razones para proponer su asimilación o, de ser el caso, descartarla.

Fuentes y Técnicas Utilizadas para la Recogida de Información

Las fuentes empleadas para recopilar la información son principalmente primarias y secundarias. Bajo esta línea, la búsqueda de datos partió por ahondar en la normativa y fundamentos jurídicos que sostienen, en el caso español, la posibilidad de acceder a datos para la identificación de usuarios, terminales y dispositivos de conectividad, sin que sea necesario que se dicte una autorización judicial, cuando se requieran en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet. Ello, teniendo como principal punto de partida la Ley Orgánica 13/2015, del 05 de octubre, que introdujo modificaciones a la Ley de Enjuiciamiento Criminal.

Esta ley, es tomada en cuenta, ya que marcó un hito en la introducción de medidas de investigación tecnológicas brindando, como su misma exposición de motivos refiere:

> Un tratamiento jurídico individualizado al acceso por agentes de policía al IMSI, IMEI, dirección IP y otros elementos de identificación de una determinada tarjeta o terminal, en consonancia con una jurisprudencia del Tribunal Supremo ya consolidada sobre esta materia. También se regula el supuesto de la cesión de datos desvinculados de los procesos de

comunicación concernientes a la titularidad o identificación de un dispositivo electrónico, a los que podrá acceder el Ministerio Fiscal o la policía judicial en el ejercicio de sus funciones sin necesidad de autorización judicial (apartado IV, párr. 11).

En atención a lo expuesto, se realizó un repaso de las limitaciones en la jurisprudencia y normativas previas que llevaron a la necesidad de introducir estas modificatorias, así como el desarrollo doctrinario y práctica jurisprudencial actual sobre estas medidas.

Habiendo cumplido con este proceso inicial, el siguiente paso -al igual que en el caso español- fue, desde la legislación peruana, establecer cómo, en el contexto de una investigación, se abordan los requerimientos de datos de identificación de usuarios, terminales y dispositivos de conectividad a las empresas proveedoras de servicios de comunicación. Para ello, fue necesario una evaluación de la legislación procesal -Código Procesal Penal-, precisando los mecanismos que se utilizan para acceder a dicha información.

Una vez identificados los procedimientos y la normativa que los sustentan, fue necesario evaluar también la legislación constitucional -Constitución Política del Perú-, analizando si los datos que se pretenden obtener están bajo la tutela de derechos constitucionales, específicamente derecho a la intimidad o inviolabilidad de las comunicaciones. De igual forma, se profundizó en la búsqueda de información emanada de instituciones gubernamentales como la Autoridad Nacional de Protección de Datos Personales, Ministerio de Transportes y comunicaciones, etc., que pueden haber determinado normativamente los alcances de protección de esta información y establecido mecanismos para su consecución.

Por último, se realizó una búsqueda general, con la finalidad de recabar diferentes posturas y, en ese mismo sentido, pronunciamientos que, sumados con las demás fuentes de información, brindaron los datos necesarios para comprender de manera específica las razones -correctas o incorrectas- por las cuales el sistema jurídico peruano obliga al Ministerio Público -en el seno de una investigación- a

solicitar ante el órgano jurisdiccional el levantamiento del secreto de las comunicaciones para obtener la identificación de usuarios, terminales y dispositivos de conectividad.

Objetivos

Para cumplir con la finalidad de la presente investigación, se han planteado los siguientes objetivos:

Objetivos generales

1. Investigar el contexto jurisdiccional por el cual se hace obligatorio, en la legislación peruana, recurrir al órgano jurisdiccional para poder acceder a datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, en contraste con la legislación española, donde es posible acceder a esta información de manera directa por parte del Ministerio Fiscal o la policía judicial en el seno de una investigación.

Objetivos específicos

1. Evaluar la funcionalidad del procedimiento de la jurisdicción procesal penal peruana para acceder a datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, frente al contexto social actual y el incremento de la delincuencia.
2. Analizar si se trastocan el derecho a la intimidad, el secreto de las comunicaciones o la Ley de Protección de Datos Personales peruana, si se autoriza a las empresas proveedoras de servicios de comunicación a brindar esta información, sin que sea necesario una orden judicial.
3. Plantear una reforma normativa en el ámbito procesal penal o cambio de criterios por parte de los operadores de justicia, en el tratamiento de la medida de investigación tecnológica ya señalada.

Contenido de la Revisión Documental

Planteamiento Español

En el caso español, como ya se mencionó, específicamente sobre los requerimientos que implicaban cesión de datos para la identificación de titulares, terminales o dispositivos de conectividad, antes de los cambios introducidos en la Ley de Enjuiciamiento Criminal por la Ley Orgánica 13/2015, estos se hacían estrictamente bajo los alcances de la Ley 25/2007, referente a la conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. La mencionada ley, además de exigir a los operadores que explotan redes públicas de comunicaciones a conservar datos necesarios para identificar al abonado o usuario registrado -entre otros, hacía énfasis en la necesidad de una autorización judicial expedida de acuerdo con los principios de necesidad y proporcionalidad, para brindar esta información a los operadores de justicia.

En atención a lo señalado, para comprender las razones por las cuales el legislador español realizó este cambio de criterios, resulta necesario hacer una pequeña pausa por la exposición de motivos del Anteproyecto de ley orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica (2015). Este anteproyecto, en el tema que nos atañe, justificó la modificatoria a razón de brindar sustento normativo a los criterios jurisprudenciales ya arraigados sobre la materia, ello en armonía con los derechos garantizados por el artículo 18 de la Constitución Española, específicamente el derecho a la intimidad personal y secreto de las comunicaciones (Rayón, 2019, pág 182; López-Barajas, 2017, pág. 97).

Este último punto es esencial, ya que a partir de este momento quedó sentado e incluso validado por el Consejo Fiscal de la Fiscalía general del Estado (2015) y el Consejo General del Poder Judicial (2015) en sus respectivos informes sobre el anteproyecto, que la cesión de los datos que identifican al titular de un

servicio y que ha cometido un delito por vía telefónica o telemática, no implicarían una vulneración al secreto de las comunicaciones. Ello, en cuanto a que este hecho no constituye en sí mismo una intervención, interceptación o registro de una comunicación, siendo, en todo caso, el derecho a la intimidad el que resultaría afectado, pero de manera mínima y soportable, ya que excede de las exigencias de la Ley de Protección de Datos y dificulta las actuaciones policiales y fiscales. Este último argumento, sustentaría que no sea necesario recurrir a la autoridad judicial para obtener esta información, máxime aun considerando que el único impedimento hasta ese momento no derivaría de la constitución sino de la ya mentada Ley 25/2007, la cual es de menor rango.

Respecto al derecho al secreto de las comunicaciones, este goza de protección constitucional en el artículo 18 inciso 3 de la Constitución Española, la cual señala: “Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial”. Asimismo, es necesario precisar -para evitar confusiones futuras- que para el ordenamiento español, este derecho protege el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como aquellos que se produzcan con independencia del establecimiento del mismo, en los que tome parte el sujeto investigado como emisor o receptor y que afecte los terminales o medios de comunicación de los que es titular (Calvo, 2017, pág. 4-5; Rayón, 2019, pág. 191; Rivero, 2017, pág. 29).

En este sentido, queda clara la distinción -ya establecida por el legislador-, en cuanto a la diferencia existente entre el acceso al contenido de la comunicación telefónica y los datos electrónicos asociados o no a un proceso de comunicación, formando parte de este último supuesto, los datos de la titularidad del servicio e incluso el número de teléfono vinculado a este (Varona, 2020, pág. 167).

Siguiendo esta línea, se ha establecido que la información referente a la titularidad de un número de teléfono o de cualquier otro medio de comunicación o los datos identificativos de estos, forman parte de la categoría de datos del abonado

(CC, 2001) que, si bien son necesarios para la prestación y facturación del servicio, no están bajo la tutela del secreto de las comunicaciones. Asimismo, resulta importante definir lo que se entiende por datos del abonado, lo cual ha sido ampliamente detallado en el Convenio sobre la Ciberdelincuencia, el cual en su artículo 18 inciso 3 precisa:

> A los efectos del presente artículo, se entenderá por «datos relativos a los abonados» cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:
>
> a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
> b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso y los datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;
> c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

Atendiendo a la naturaleza de la información que engloba esta categoría, si se circunscribe únicamente como datos de abonado a aquellos datos de identificación de la persona física o jurídica registrada con vinculación contractual para hacer uso y disfrutar del servicio, estaríamos ante un contenido susceptible de protección del artículo 18 inciso 4 de la Constitución Española, el cual señala: “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”. Este artículo, no considera -como en artículo 18 inciso 3- de manera explícita la necesidad de resolución judicial, sino que traslada a un rango legal los límites de acceso, en atención a garantizar el derecho a la intimidad personal. Sin embargo, es necesario

aclarar que, ciertos datos del abonado conforme han sido expuestos en el Convenio sobre la Ciberdelincuencia, se encuentran ligados a la propia comunicación al establecer el origen y destino de esta, su momento y duración, los cuales son generados mientras la comunicación se encuentra en curso, por lo que, para estos, sí resultaría necesario una autorización judicial (Calvo, 2017, pág. 8).

Al haber establecido que el mecanismo adecuado para la tutela de la información relativa a los datos del abonado, específicamente los de su identificación, sería una norma con rango de ley, se puede precisar que la norma que resulta más idónea para esta tutela sería la Ley de Protección de Datos Personales. Al respecto, es necesario precisar que, en el contexto de la investigación de un delito, es de aplicación la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Esta ley, aparte de establecer los alcances del tratamiento de datos para estos fines, dentro de su redacción, en su artículo 13, hace referencia al tratamiento de cierta categoría de datos especiales, limitándolos a ciertas excepciones:

> El tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud o a la vida sexual o a la orientación sexual de una persona física, sólo se permitirá cuando sea estrictamente necesario, con sujeción a las garantías adecuadas para los derechos y libertades del interesado y cuando se cumplan alguna de las siguientes circunstancias:
>
> a. Se encuentre previsto por una norma con rango de ley o por el Derecho de la Unión Europea.
> b. Resulte necesario para proteger los intereses vitales, así como los derechos y libertades fundamentales del interesado o de otra persona física.

c. Dicho tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos.

Como es de apreciar, los datos a los que hace referencia este artículo forman parte de datos especialmente protegidos, los cuales gozan de cierta excepcionalidad para ser recabados, tratados y cedidos, limitándose esto al marco de una investigación, sin perjuicio del control jurisdiccional que se pudiera tener. Por otro lado, los datos del abonado referidos a la titularidad de un número de teléfono o de cualquier otro medio de comunicación o los datos identificativos de estos, si bien son datos personales, no forman parte de los datos considerados como sensibles o especialmente protegidos y, por tanto, son susceptibles de ser tratados conforme a la normativa ya señalada y siguiendo los lineamientos de su conservación conforme a la Ley 25/2007.

De esta manera, ya habiendo determinado el sustento normativo que habilita a la Policía Judicial y al Ministerio Fiscal a requerir estos datos directamente a los prestadores de servicios, conforme a lo estipulado en el artículo 588 ter m de la Ley de Enjuiciamiento Criminal, objeto de la presente investigación. Es necesario, hacer una pequeña evaluación de los alcances que ha establecido la doctrina para esta medida y un breve ejemplo del desarrollo jurisprudencial que ha significado.

Este artículo, por su estructura y practicidad, no ha merecido un desarrollo doctrinario muy amplio, sin embargo, ha estado sujeto a cuestionamientos en lo que respecta al alcance de su aplicación. Para autores como David Calvo (2017), Gorgonio Martínez (2020) y Montoro & Sánchez (2021), dota de autonomía al Ministerio fiscal y la Policía Judicial en supuestos que resultan ser poco invasivos a los derechos contenidos en el artículo 18 de la Constitución Española -siendo esta razón de la prescindencia de la garantía del control judicial- amparando aquellas peticiones de datos orientadas a determinar la identificación del titular o del dispositivo de comunicación, siempre que no se trate de datos relacionados a procesos de comunicación.

Asimismo, para comprender su alcance, David Calvo (2017, pág. 27), traslada en su obra las Actas del Comité Técnico de la Comisión Nacional de Coordinación de Policía Judicial de fechas 15 de julio y 24 de noviembre de 2016, en las cuales las compañías telefónicas precisan los datos sobre los cuales es aplicable esta normativa, siendo:

- Cuando a partir de los datos de identificación del individuo se les solicita el número de la línea telefónica, el IMSI y el IMEI.
- Cuando a partir del IMSI de la línea telefónica se les solicita el número de la línea telefónica y los datos de identificación del titular.
- Cuando a partir del IMEI del terminal se les solicita el número de la línea telefónica y los datos de identificación del titular que consten en sus bases de clientes.

Sin embargo, se ha mostrado cierta reticencia por parte de las compañías telefónicas cuando se les requiere cuál es la tarjeta SIM concreta con que está funcionando un determinado terminal de telefonía móvil o, en sentido contrario, qué móvil concreto está siendo utilizado para el funcionamiento de una tarjeta SIM determinada. Estas empresas, argumentan su negativa en que solo se tiene esta información cuando la empresa ha proveído conjuntamente ambos elementos, pues, en otros contextos, sería necesario acceder a los registros derivados de las conexiones con la red efectuadas desde dicho dispositivo, momento en el que el operador puede captar no solamente el IMSI de la tarjeta sino también el IMEI identificativo del terminal físico utilizado como soporte. En este sentido, para acceder a este tipo de solicitudes, para las empresas resulta necesario llevar a cabo una búsqueda en las bases de datos en que se almacena el tráfico cursado por dicha línea móvil, lo cual ya hace necesaria la autorización judicial conforme a la Ley 25/2007 (UCRINFO, 2019, pág. 5).

Respecto a esta circunstancia, la Unidad de Criminalidad Informática, planteó lo siguiente:

> Los códigos de identificación IMEI e IMSI, cuyo objeto y finalidad es la identificación respectivamente del terminal físico y del usuario del servicio de comunicación, tienen la consideración de datos sobre abonados siempre que la solicitud/facilitación de los mismos se haga como dato independiente y aislado o desvinculado de cualquier otra información sobre los procesos comunicativos en que dichas numeraciones hayan podido ser utilizadas (UCRINFO, 2019, pág. 8).

Por lo tanto, acorde a lo expuesto, concluyen en que la sesión de estos datos, ya sea adquiridos por los prestadores de servicios de manera aislada o vinculados entre si, forman parte de los alcances del artículo 588 ter m de la Ley de Enjuiciamiento Criminal. Sobre esta línea, se debe resaltar que, este criterio ha sido respaldado por la Agencia Española de Protección de Datos en su Informe Nº 2021-0030, de 30 de noviembre de 2021, donde señala lo siguiente:

> … el acceso por parte de las FCS y el Ministerio Fiscal a los datos referidos a la vinculación entre el IMEI del dispositivo dónde se usa la SIM duplicada y la propia SIM salvo mejor criterio de aquellos organismos o instituciones con competencias en este ámbito, no requerirá autorización judicial siempre y cuando la petición no esté vinculada a un proceso de comunicación concreto, en cuyo caso, se aplicaría la Ley 25/2007 de 18 de octubre.

De esta manera, la autoridad competente deja zanjada la disyuntiva existente entre las empresas prestadoras de servicio de las telecomunicaciones y el Ministerio Fiscal y Policía Judicial, con lo que se ha podido establecer el rango de datos que pueden ser cedidos en aplicación del artículo 588 ter m de la Ley de Enjuiciamiento Criminal.

Por último, a modo ilustrativo, se expone un ejemplo de aplicación de esta medida de investigación, lo cual nos permite apreciar una de las utilidades y criterio jurisprudencial empleado en la atención de estos requerimientos:

La Sección Segunda de la Audiencia Provincial de Cáceres en el Recurso de Apelación N° 726/2017, en el contexto de un robo violento, en el que los autores del hecho se apoderaron de un teléfono móvil. En la investigación, se requirió a distintas compañías de telefonía que brinden las tarjetas SIM que se hayan insertado en el terminal con IMEI NUM000 en un periodo de espacio y tiempo determinado. Sobre este punto, resulta importante el fundamento esgrimido por el órgano jurisdiccional en el considerando segundo, donde expone lo siguiente:

> Al respecto de esta información hemos declarado recientemente (recurso de apelación 807/2017) que respecto de la solicitud de información sobre los números de abonados asociados a determinados IMEIS, así como los datos de identidad que se refieran a aquéllos, entendemos que no se trata propiamente de una intervención judicial de un terminal móvil, ni la observación ni grabación de las conversaciones, ni tan siquiera la cesión de los datos asociados, llamadas, posición, etc.: En similar sentido señala la Audiencia Provincial de Cádiz, Sección 3ª, en su Auto de 17 de enero de 2017, que tal injerencia no afecta al contenido del secreto de las comunicaciones, ni tan siquiera creemos afecte materialmente al derecho a la intimidad, insistimos no se pide ningún dato asociado, los datos recabados no pueden permitir extraer conclusiones sobre la vida privada de las personas a las que afecten y de ahí que si la policía puede directamente conforme al art 588 ter m dirigirse a las operadoras para pedir la identificación de un titular de un número, o el número de un terminal, cuanto más dicha diligencia podrá ser acordada por la autoridad judicial a solicitud policial, donde las garantías quedan reforzadas, se trata de una injerencia mínima y conforme al principio de especialidad, precisa para la determinación de los autores de un delito, idónea además pues permite identificar al poseedor de un determinado terminal ilegítimamente arrebatado a su dueño y por ende necesaria, al no contar con otro medio alternativo para el esclarecimiento del hecho denunciado además de proporcionada, proporcionalidad que medimos considerando, insistimos en ello, la mínima injerencia que ocasiona.

Evaluación del Contexto Peruano

Como se precisó al inicio de esta investigación, en la práctica jurisdiccional peruana, para acceder a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, es necesario postular un requerimiento ante el Poder Judicial, con la finalidad de que autorice a las empresas telefónicas a brindar esta información. Es usual, que todos los requerimientos relacionados con las telecomunicaciones se presenten ante el órgano jurisdiccional al amparo de tres artículos del Código Procesal Penal:

El primero, es el artículo 188 referente al abordaje de la prueba documental y le procedimiento para requerir informes, ya sea de registros oficiales o privados, siendo su tenor el siguiente:

> El Juez o el Fiscal durante la Investigación Preparatoria podrá requerir informes sobre datos que consten en registros oficiales o privados, llevados conforme a Ley. El incumplimiento de ese requerimiento, el retardo en su producción, la falsedad del informe o el ocultamiento de datos, serán corregidos con multa, sin perjuicio de la responsabilidad penal correspondiente, y de la diligencia de inspección o revisión y de incautación, si fuera el caso.

El segundo artículo, el 230 inciso 1, está relacionado con la intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles, siendo su contenido el siguiente:

> El Fiscal, cuando existan suficientes elementos de convicción para considerar la comisión de un delito sancionado con pena superior a los cuatro años de privación de libertad y la intervención sea absolutamente necesaria para proseguir las investigaciones, podrá solicitar al Juez de la Investigación Preparatoria la intervención y grabación de comunicaciones telefónicas, radiales o de otras formas de comunicación...

Por último, el tercer artículo es el 253 inciso 1 y 2, el cual expresa los preceptos generales en la atención de medidas de coerción procesal, exponiendo lo siguiente como principios y finalidad:

1. Los derechos fundamentales reconocidos por la Constitución y los Tratados relativos a Derechos Humanos ratificados por el Perú, sólo podrán ser restringidos, en el marco del proceso penal, si la Ley lo permite y con las garantías previstas en ella.
2. La restricción de un derecho fundamental requiere expresa autorización legal, y se impondrá con respeto al principio de proporcionalidad y siempre que, en la medida y exigencia necesaria, existan suficientes elementos de convicción.

Teniendo esta base normativa en la atención de estos requerimientos, queda claro que la necesidad de solicitar ante el Poder Judicial la autorización para que los prestadores de servicios de telecomunicaciones, las empresas de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información; brinden los datos de la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, el número de teléfono o los datos identificativos de cualquier medio de comunicación; no nace del mismo cuerpo normativo del Código Procesal Penal, sino resulta ser una imposición legal específica de la materia, la cual está relacionada con la protección de ciertos derechos fundamentales aparados por la Constitución Política del Perú.

En atención a este último punto, antes de abordar la normativa específica que desarrolla la protección de esta información, es necesario identificar sobre qué derecho fundamental en particular recae la tutela de la misma. En este sentido, hay dos posibles derechos reconocidos por la carta magna peruana que podrían estar vinculados a los datos para la identificación de titulares, terminales o dispositivos de conectividad. Ambos, pertenecen al artículo 2, el cual enumera de manera taxativa los derechos fundamentales de la persona, debiendo precisar que no son los únicos derechos reconocidos atendiendo a la cláusula de los derechos implícitos

(Sentencia, 2005a). El primero, sería el artículo 2 inciso 6, el cual refiere que: “Toda persona tiene derecho: A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar”. El segundo, es el artículo 2 inciso 10, que precisa lo siguiente: “Toda persona tiene derecho: Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados…”.

Respecto a este último, el derecho al secreto y a la inviolabilidad de las comunicaciones, para la doctrina y jurisprudencia peruana, se garantiza que el contenido de las comunicaciones solo puede ser conocida por los intervinientes, no limitándose al contenido sino al proceso mismo de comunicación, siendo estos, cualquiera de los posibles medios de intercambio de información e ideas que se pueda dar entre dos o más personas, ampliando su espectro a todos aquellos instrumentos de desarrollo tecnológico que se presenten en el futuro y limitando su apertura, incautación, interceptación o intervención, a mandato motivado por el juez (Sentencia, 2003; Rubio, 2013, pág. 403). Como es de apreciar, los datos de identidad de un determinado usuario de una empresa prestadora de servicios de la comunicación no están bajo el amparo de este derecho fundamental, ya que la información que se pretende obtener no corresponde al proceso de comunicación.

Por otro lado, situación diferente es la que se presenta en el artículo 2 inciso 6 de la carta magna peruana, el cual reconoce el derecho a la autodeterminación informativa. Este derecho, ha sido objeto de pronunciamiento por el Tribunal Constitucional, el cual lo define de la siguiente manera:

> El derecho a la autodeterminación informativa consiste en la serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos. 5. De esta forma se busca proteger a la persona en sí misma, no únicamente en los derechos que conciernen a su esfera personalísima, sino a la persona en la totalidad de ámbitos. Por ende, no puede identificarse a la

> autodeterminación informativa con el derecho a la intimidad, personal o familiar, ya que, mientras éste protege el derecho a la vida privada, el derecho a la autodeterminación informativa busca garantizar la facultad de todo individuo de poder preservarla ejerciendo un control en el registro, uso y revelación de los datos que le conciernen, ya sea que la información se encuentre en disposición de entidades públicas, o sea de carácter privado… (Sentencia, 2014).

Por lo tanto, queda claro que los datos de identificación de usuarios, terminales y dispositivos de conectividad, los cuales son almacenados en bancos de datos por las empresas prestadoras de servicios de las telecomunicaciones en el contexto de un contrato de prestación de servicios, quedan bajo los alcances del derecho a la autodeterminación informativa.

Sobre esta línea, es necesario precisar que, este derecho encuentra su desarrollo normativo y protección en la Ley N° 29733, Ley de protección de datos personales, el cual garantiza los derechos de los ciudadanos al acceso a sus datos personales, rectificación o cancelación de estos u oposición en su tratamiento (Mubarak, 2017); Sin embargo, es necesario aclarar que dentro de la estructura de la norma, específicamente en el inciso 2 del artículo 3, se precisa que los preceptos contenidos en esta ley no son de aplicación "… para el desarrollo de actividades en materia penal para la investigación y represión del delito". Asimismo, en el inciso 1 del artículo 14, la misma ley precisa como una de las limitaciones al consentimiento para el tratamiento de datos personales; "Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias". Con lo señalado, se puede concluir, que la ley se reserva para casos no cubiertos por leyes específicas y frente al requerimientos o tratamientos de terceras personas o entidades públicas, cuando no sea en el ámbito de sus atribuciones, lo cual se ampliará más adelante.

Por lo expuesto, habiendo establecido la protección constitucional sobre la información objeto de la presente investigación y las excepciones para su

tratamiento con base en la Ley de Protección de Datos Personales; se hace necesario definir la normativa sobre la materia que impide que esta sea brindada de manera libre al Ministerio Publico cuando es requerida en le contexto de una investigación. Bajo esta premisa, para encontrar el sustento que hace imperativo acudir al órgano jurisdiccional, se tiene que hacer una remisión a la normativa emanada del sector de las telecomunicaciones, específicamente por el Ministerio de Transportes y Comunicaciones [MTC].

Este órgano estatal, en cuanto a la protección de datos personales en el contexto de la prestación de los servicios de las telecomunicaciones, en el tema que nos ocupa, ha realizado las siguientes precisiones:

La primera, está contenida en el Decreto Supremo Nº 020-2007-MTC, el cual aprueba el Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones. Esta normativa señala, en su artículo 13 lo siguiente:

> … Los concesionarios de servicios públicos de telecomunicaciones están obligados a salvaguardar el secreto de las telecomunicaciones y la protección de datos personales, adoptar las medidas y procedimientos razonables para garantizar la inviolabilidad y el secreto de las comunicaciones cursadas a través de tales servicios, así como mantener la confidencialidad de la información personal relativa a sus usuarios que se obtenga en el curso de sus negocios, salvo consentimiento previo, expreso y por escrito de sus usuarios y demás partes involucradas o por mandato judicial.

La segunda precisión, se encuentra en la Resolución Ministerial N° 111-2009-MTC/03, norma de desarrollo del artículo 13 del Decreto Supremo antes mencionado, el cual señala textualmente en el artículo 8 lo siguiente: “De la vulneración a la protección de datos personales. Se atenta contra la protección de la información personal relativa a los abonado o usuarios cuando ésta es entregada a terceros, salvo las excepciones previstas en la legislación vigente…”.

Asimismo, también el Organismo Supervisor de Inversión Privada en Telecomunicaciones [OSIPTEL], respecto a la protección de los datos personales de los usuarios de los servicios públicos de telecomunicaciones, ha precisado en el artículo 67-C del Texto Único Ordenado de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones - Resolución de Consejo Directivo Nº 138-2012-CD-OSIPTEL, lo siguiente:

> El abonado tiene derecho a gozar de una protección especial en cuanto al manejo confidencial y privado de los datos personales que haya proporcionado a la empresa operadora, sea al momento de la contratación o durante la provisión del servicio. Asimismo, el abonado podrá ejercer, en cualquier momento, los derechos de acceso, rectificación, cancelación y oposición de sus datos mediante cualquiera de los mecanismos de contratación a que se refiere el artículo 118. (…) Asimismo, la empresa operadora solo podrá utilizar los referidos datos para los fines específicos asociados a la prestación del servicio público de telecomunicaciones que ha contratado.

En este sentido, al evaluar los extractos de las normas citadas, se puede inferir que la necesidad de solicitar al juez de garantías la emisión de una resolución para autorizar a las empresas de telefonía a brindar información sobre la identidad del titular del servicio, queda condicionada principalmente por estas normativas, que postulan la exigencia del consentimiento del titular o una ley que autorice su tratamiento, o en su defecto, como es el caso en cuestión, un mandato judicial.

Por último, con relación en este apartado, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales [DGTAIPD], ha emitido el 30 de setiembre del 2021, la Opinión Consultiva N° 040-2021-JUS/DGTAIPD, referente a la posibilidad de entrega de información de abonados (identidad de titulares de números telefónicos y titulares de IP) al Ministerio Público, en virtud de la adhesión del Perú al Convenio de Budapest.

Este es un aspecto muy importante, ya que el organismo formalmente autorizado, en uso de las atribuciones conferidas conforme a lo establecido por el artículo 24 de la Ley N° 29733, Ley de Protección de Datos Personales y por el artículo 74 de su reglamento, ha emitido un pronunciamiento que, en teoría, establecería los parámetros para el acceso a esta información.

En el documento en mención, la Unidad de Cooperación Judicial Internacional y Extradiciones de la Fiscalía de la Nación [UCJIE], realiza la consulta en su deber de cooperación en el intercambio de información de manera directa en el marco de investigaciones penales, en su condición de integrante de la Asociación Iberoamericana de Ministerios Públicos y en atención a la reciente suscripción de Perú al Convenio sobre la Ciberdelincuencia; pone en conocimiento de la DGTAIPD que ha recepcionado requerimientos por parte de otros estados respecto a la titularidad de números telefónicos y de IP, los cuales no han podido ser tramitados ya que las empresas de telefonía precisan que para brindar esta información, conforme a la Ley de Protección de Datos Personales, necesitan primero una autorización judicial.

Al respecto, la DGTAIPD ha mostrado su negativa a que las empresas de telefonía brinden de manera directa al Ministerio Público, información de abonados, como nombres y apellidos de los titulares de números telefónicos y titulares de IP, bajo los siguientes argumentos:

- Señala que estos datos constituyen información confidencial al tratarse de datos personales, cuya publicidad puede afectar la intimidad personal del titular.
- Precisa que el Código Procesal Penal, ante las medidas que limitan derechos fundamentales requiere que sean dictadas por la autoridad judicial o a través de una ley que lo permita y con las garantías previstas.
- Considera que las disposiciones del Convenio de Budapest no habilitan legalmente al Ministerio Público a acceder a esta información sin haber

adoptado las medidas legislativas pertinentes, conforme a lo establecido en su artículo 18 inciso 1 literal b.

Asimismo, concluye su análisis señalando que, las empresas concesionarias de servicios públicos de telecomunicaciones solo podrán realizar tratamiento de la información de abonados, siempre que el titular haya otorgado consentimiento, bajo autorización judicial o mandato legal expreso que así lo ordene. Asimismo, recomienda al Ministerio público evaluar la necesidad de realizar una adecuación legislativa que habilite a acceder a la información de abonados, permitiendo de esta manera actuar en el marco de las acciones de cooperación internacional del Convenio de Budapest.

No obstante, a las razones expuestas por la DGTAIPD, se considera que la posición tomada es cuestionable, ya que no se habría realizado una evaluación integral de la normativa inmersa en este proceso, aunado a la confusión de términos en cuanto a la calidad de datos solicitados, debiendo haber establecido diferencias entre los mismos, ya que ambos merecen protección diferenciada; lo cual será parte del objeto de análisis que se realizará a continuación.

Análisis e Interpretación Referentes a la Información Expuesta

De la evaluación realizada en el apartado anterior, es necesario precisar que, se ha podido colegir que el procedimiento de la jurisdicción procesal penal peruana para acceder a datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad, frente al contexto social actual y el incremento de la delincuencia resulta disfuncional.

Para iniciar con el análisis, debemos tener presente que la investigación del delito por parte del Ministerio Público debe estar destinada a ejercitar la acción penal, para lo cual deberá obtener los elementos de convicción necesarios para acreditar los hechos delictivos, así como para identificar a los autores o partícipes en su comisión, conforme lo señalado en el artículo 65 del Código Procesal Penal. En el mismo sentido, dentro de un proceso, el mismo cuerpo normativo, en su

artículo 330 inciso 2, exige para lograr este fin que se deban "…realizar los actos urgentes o inaplazables destinados a determinar si han tenido lugar los hechos objeto de conocimiento y su delictuosidad, así como asegurar los elementos materiales de su comisión, individualizar a las personas involucradas en su comisión…".

Como se puede apreciar, uno de los aspectos fundamentales de toda investigación fiscal es determinar la identidad de la persona que ha cometido un ilícito, esto comporta, la necesidad de dirigir el proceso desde su inicio contra una persona cierta y plenamente identificada e individualizada, siendo necesario la realización de actos de investigación dirigidos a precisar el nombre de la persona a la cual se le imputa la comisión de un hecho delictivo, lo que también garantiza el derecho del imputado a defenderse de los cargos formulados en su contra (Defensoría del Pueblo, 2009). Es por este motivo, que la norma procesal que rige este procedimiento, en su artículo 337 inciso 3 literal b, autoriza dentro de las diligencias de investigación preparatoria, a que el fiscal pueda "Exigir informaciones de cualquier particular o funcionario público, emplazándoles conforme a las circunstancias del caso".

Bajo este contexto, resulta entonces necesario que el Ministerio Público -como titular de la acción penal- cuente con los medios necesarios para ejecutar dicho fin, y no encuentre en su ejercicio limitaciones que no tienen sustento constitucional o mínimamente legal, máxime aún si responden a un objetivo de interés general, el cual representa la lucha contra la delincuencia y, propiamente, la seguridad pública.

En este sentido, resulta cuestionable la motivación expuesta por la DGTAIPD en la Opinión Consultiva N° 040-2021-JUS/DGTAIPD -la cual engloba en gran medida nuestra problemática, para descartar la posibilidad de que las empresas prestadoras de servicios de las telecomunicaciones brinden de manera directa al Ministerio Público la información de sus abonados, por lo que resulta necesario

hacer precisiones en los puntos tratados, al considerar que no se ha realizado una interpretación y ponderación adecuada de la normativa circundante en esta materia.

Se debe iniciar precisando que, si bien la UCJIE hizo la consulta de manera general, poniendo en la misma categoría de datos aquellos relacionados con la identidad de titulares de números telefónicos y aquellos que permiten la identificación del titular del servicio mediante el número IP, correspondía a DGTAIPD, al ser el ente especializado en la materia, realizar la clara distinción que tienen estas categorías de datos, atendiendo a la diferente protección constitucional que merecen.

En el caso de la IP, este es un protocolo para el envío y recepción de datos a través de una red de paquetes conmutados. El proveedor de servicios de internet asigna un número de IP al usuario cuando empieza a usar el servicio y es el que permite su identificación e interacción (Miró, 2012, pág. 307; Calvo López, 2017, pág. 12). Como es de apreciar, si bien el operador asigna un IP -en la mayoría de los casos- a un usuario determinado, este va conexo al proceso de comunicación del internauta, siendo obtenida –algunas veces de manera pública- cuando la comunicación está en curso o ya ha finalizado, ya sea en el contexto de intercambio de archivos P2P, el envío de un correo electrónico, comunicaciones realizadas por redes sociales, etc. Asimismo, se debe precisar que, si bien la obtención de una dirección IP puede ser develada por el mismo usuario dentro de su interacción en la red, en la mayoría de los casos formará parte de la comunicación realizada entre dos o más personas, lo que ya implica que forme parte de los datos relativos al tráfico, es decir, al proceso mismo de comunicación.

Sobre este último aspecto, el Convenio sobre la Ciberdelincuencia, en su artículo 1 literal d, ha definido a los datos relativos al tráfico como:

> Todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora,

la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Por lo tanto, queda claro que si bien el conocimiento de la dirección IP por terceros -en muchos casos- se produce por acción voluntaria del usuario al ser un dato público propio de su interacción en la red, para que sea vinculada a un usuario específico, cuando se da en el contexto de un proceso de comunicación, se hace necesario que su cesión por parte de las empresas sea autorizado por el juez de garantías, por resultar una intromisión a los derechos protegidos por el artículo 2 inciso 10 de la constitución política del Perú –el secreto e inviolabilidad de las comunicaciones.

Caso diferente sería los datos relacionados con la identidad de titulares de números telefónicos, debiendo ampliar el alcance de esta evaluación -por ser la finalidad de esta investigación- no solo a los que vinculan un determinado número telefónico con un usuario específico, sino también al usuario con cualquier otro medio de comunicación, así como en sentido inverso, identifiquen el número de teléfono o los datos identificativos de cualquier medio de comunicación con un determinado usuario; incluyendo, por ende, la vinculación del IMEI y IMSI.

Al respecto, para evitar ser repetitivos con la información a exponer, ya en el apartado del Contenido de la Revisión Documental -específicamente en el Planteamiento Español- hemos abordado lo que el Convenio sobre la Ciberdelincuencia, en su artículo 18 inciso 3, define como datos relativos a los abonados. En razón a ello, si hablamos específicamente del número telefónico, el código IMEI de un equipo móvil y el código IMSI integrado en la tarjeta SIM, nos estamos refiriendo a datos propiamente del abonado, los cuales no están ligados a un proceso de comunicación, recayendo su tutela bajo los alcances del artículo 2 inciso 6 de la constitución política del Perú –la autodeterminación informativa.

Siguiendo esta línea, es necesario aclarar que los datos a los cuales hacemos mención forman parte de la contratación del servicio y son almacenados por las empresas de telefonía en el ejercicio de sus operaciones, conforme a lo

señalado en la Resolución de Consejo Directivo Nº 138-2012-CD-OSIPTEL. Esta normativa, en el quinto párrafo de su artículo 11, exige a las empresas operadoras llevar un registro actualizado de sus abonados bajo todas las modalidades de contrato, exigiendo que el registro sea independiente. Asimismo, en la misma línea, la normativa de OSIPTEL también exige en su artículo 11-B que, independientemente del registro de la información almacenada a la que se acaba de hacer mención, la operadora de servicios móviles deberá tener un registro de todos los equipos terminales móviles a través de los cuales presta el servicio, incluyendo los no comercializados por ella, exigiendo que el registro posea: código IMEI del equipo terminal móvil o número de serie electrónico que lo identifica; marca del equipo terminal móvil; modelo del equipo terminal móvil; código IMSI que activa el equipo terminal móvil; tipo de abonado; modalidad de contrato y estado del servicio. Cabe precisar, que estos datos forman parte de la lista blanca del Registro Nacional de Equipos Terminales Móviles para la Seguridad, sobre el cual se ahondará más adelante.

Por lo expuesto, si bien no se hace una mención específica en la normativa abordada, queda claro que estos bancos de datos quedan bajo los alcances de la Ley de Protección de Datos Personales y, como se hizo mención en el apartado anterior, si bien esta ley es aplicable para los tratamiento realizados por parte de las empresas prestadoras del servicio de las telecomunicaciones, no es aplicable para el desarrollo de actividades en materia penal para la investigación y represión del delito -artículo 3 inciso 2.

Sin embargo, la DGTAIPD, valiéndose de normativas emanadas por el MTC como el Decreto Supremo Nº 020-2007-MTC y la Resolución Ministerial N° 111-2009-MTC/03, hace énfasis en que las mismas -para el tratamiento de estos datos y preservar su confidencialidad- imponen la necesidad del consentimiento del titular o una ley que autorice su tratamiento o un mandato judicial que autorice su cesión. No obstante, es necesario que estas normas sean interpretadas, por ser de rango inferior, sobre la base de la Ley de Protección de Datos Personales atendiendo al principio de especialidad. Esta ley, respecto al contenido del consentimiento del

titular de datos personales, precisa que este no se requiere para su tratamiento, cuando estos datos se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias -artículo 14 inciso 1. De igual forma, en cuanto a la confidencialidad, esta ley si bien establece el deber del titular del banco de datos a resguardarla, lo libera de esta obligación cuando medien razones fundadas relativas a la seguridad pública -artículo 17.

Con lo expuesto, se puede concluir que se excluye al titular del banco de datos de la necesidad del consentimiento del titular de los datos, así como de su deber de confidencialidad, para el tratamiento efectuado por el Ministerio Público en atención a las facultades constitucionalmente conferidas conforme al artículo 159 de la carta magna, y las funciones atribuidas acorde al artículo 1 de su Ley Orgánica, la cual precisa:

> El Ministerio Público es el organismo autónomo del Estado que tiene como funciones principales la defensa de la legalidad, los derechos ciudadanos y los intereses públicos, la representación de la sociedad en juicio, para los efectos de defender a la familia, a los menores e incapaces y el interés social, así como para velar por la moral pública; la persecución del delito y la reparación civil…

En este contexto, también es necesario precisar que la DGTAIPD en su opinión consultiva, también pone como limitación al acceso directo por parte del Ministerio Público a los datos de identificación del titular de una línea telefónica, que es el mismo Código Procesal Penal, el que requiere que las medidas que limitan derechos fundamentales sean dictadas por la autoridad judicial o a través de una ley que lo habilite, conforme a los artículos VI del título preliminar y el 253 inciso 2.

Para hacer frente a esta precisión, es necesario aclarar que los artículos mencionados son una referencia expresa a las medidas limitativas de derechos, las cuales, por su alto grado de afectación a los derechos fundamentales de la persona, han sido expresamente autorizados por ley, e incluso, establecido procedimientos

para su obtención, alcances y limitaciones, conforme lo requiere la misma norma procesal, reservando su resolución a la autoridad jurisdiccional.

Es así, que Ley Nº 27379, de procedimiento para adoptar medidas excepcionales de limitación de derechos en investigaciones preliminares, además de precisar los lineamientos para sus requerimientos ante el Poder judicial, considera en su artículo 2 las siguientes medidas: Impedimento de salida del país o de la localidad en donde domicilia el investigado o del lugar que se le fije, incomunicación, secuestro y/o incautación de los objetos de la infracción penal o los instrumentos con que se hubiere ejecutado así como los efectos, embargo u orden de inhibición para disponer o gravar bienes, levantamiento del secreto bancario y de la reserva tributaria, exhibición y remisión de información en poder de instituciones públicas o privadas, allanamiento de inmuebles o lugares cerrados fuera de los casos de flagrante delito o de peligro inminente de su perpetración, Inmovilización de bienes muebles y clausura temporal de locales. De igual forma, se tiene que en el propio Código Procesal Penal, se encuentran las siguientes medidas de coerción personal: detención policial, arresto ciudadano, detención preliminar judicial, prisión preventiva, comparecencia, detención domiciliaria, internación preventiva, impedimento de salida del país y suspensión preventiva de derechos; así como medidas reales como: el embargo, orden de inhibición, desalojo preventivo, medidas anticipadas como la pensión anticipada de alimentos e incautación (Valderrama, 2021).

De esta manera, se ha visto conveniente enumerar extensivamente lo que la ley y doctrina considera como medidas limitativas de derechos, ya sea personales o reales, atendiendo al alto grado de injerencia estatal que suponen estas medidas sobre las libertades reconocidas constitucionalmente. Sobre este punto, Cesar San Martín (2020, pág. 512) precisa que, si bien el Código Procesal Penal ha previsto un amplio esquema de actos procesales que limitan derechos fundamentales, en su estructura, ha distinguido diferéntes márgenes de intervención de los operadores de justicia -policía, fiscal y juez, reconociendo, por tanto, afectaciones de grado leve, medio e intenso de los derechos fundamentales, ello:

> … a fin de articular de una manera adecuada la autonomía y rol de director de la investigación del Ministerio Público con la salvaguarda de los derechos fundamentales, reconociendo a la Fiscalía un desarrollo autónomo de las acciones básicas relativas a sus competencias y que no supongan una amenazamedia o intensa para la dignidad del individuo y los derechos fundamentales que la garantizan, y de otro aplicar la máxima in dubio pro libertate para que las afectaciones medias e intensas requieran el control previo de necesidad y proporcionalidad del juez de la Investigación Preparatoria.

Esta mención es importante, ya que -como es de apreciar- la DGTAIPD ha realizado un interpretación sumamente extensiva y desproporcionada de la norma procesal, no habiendo realizado una adecuada ponderación respecto a la calidad de información sobre la cual se pretende el acceso, frente a las facultades y atribuciones conferidas legal y constitucionalmente al Ministerio Público para el ejercicio de sus funciones.

En este punto, se entrevé que se estaría frente a dos principios constitucionales que entran en conflicto, por lo tanto, con el fin de dilucidar esta controversia, se debe empezar señalando que para el Tribunal Constitucional:

> Ningún derecho fundamental, en efecto, puede considerarse ilimitado en su ejercicio. Los límites que puede imponérseles son intrínsecos o extrínsecos. Los primeros son aquellos que se deducen de la naturaleza y configuración del derecho en cuestión. Los segundos, en cambio, se deducen del ordenamiento jurídico, cuyo fundamento se encuentra en la necesidad de proteger o preservar otros bienes, valores o derechos constitucionales (Sentencia, 2005b).

En este sentido, por un lado, se tiene los principios constitucionales emanados de la actividad propia del Ministerio Público, en su deber de comprobación de los hechos, para lo cual está facultado a ejecutar actos de investigación orientados -entre otras cosas- a descubrir a las personas involucradas

en un hecho ilícito, con la finalidad de que estas conductas no queden impunes y se satisfaga y concretice el principio del interés general en la investigación y persecución del delito (Sentencia, 2014). En el otro extremo, tenemos al principio constitucional relacionado a la autodeterminación informativa, con lo cual, los datos que vinculan a un usuario con un número telefónico, el código IMEI de un equipo móvil y el código IMSI integrado en la tarjeta SIM; forman parte de los datos protegidos por el derecho de la persona a mantener su vida privada en reserva, brindándole la facultad de preservarla al ejercer un control en el registro, uso y revelación de sus datos, debiendo precisar que, la vida privada al ser un concepto muy amplio, se considera afectada cuando la información atenta contra la libertad y dignidad de la persona (Gaceta Jurídica, 2005). Asimismo, la medida que se postula es que, el Ministerio Publico en el contexto de la investigación de un delito, requiera a las empresas prestadoras del servicio de la comunicación a brindar, sin autorización judicial, los datos de identificación de usuarios, terminales y dispositivos de conectividad.

En este punto, es necesario precisar que el Tribunal Constitucional, ha precisado que, para establecer la legitimidad constitucional de una limitación al ejercicio de los derechos fundamentales, además de la observancia del principio de legalidad, deben concurrir además el requisito de proporcionalidad y razonabilidad (Sentencia, 2005c), los cuales gozan de una unidad esencial al suponer el rechazo de todo acto arbitrario en respecto de los derechos constitucionales (Castillo, 2005; pág. 10-11). Bajo esta línea, Luis Castillo (2005) precisa que, para poder determinar si existe una relación de equilibrio o de adecuada correspondencia entre la afectación que llegaría a sufrir el derecho constitucional y la conservación de un bien o interés público que aparece precisamente como causa de esa afectación, es necesario someter la medida a un triple juicio de proporcionalidad, el cual está conformado por el juicio de idoneidad, el juicio de necesidad y el juicio de proporcionalidad sensu estricto.

Sobre esta premisa, si aplicamos este triple juicio al caso en concreto, tenemos que, aplicado el juicio de idoneidad, la medida propuesta resulta idónea al

formar parte de los actos de investigación del Ministerio Público con la finalidad de ejercitar la acción penal, siendo adecuada para la determinación de la identidad del presunto delincuente, al estar frente a casos donde se cuenta con información limitada -sólo un número de celular o IMEI- y las nuevas tecnologías, en especial el uso de teléfonos móviles, proporcionan una fuente importante de información para investigar cualquier delito, no solamente los telemáticos (Calvo, 2017, pág. 9).

Respecto al juicio de necesidad, encontramos que esta medida es necesaria al no contar en la normativa procesal con otra igualmente eficaz, ello ante la cualidad de la información requerida, ya que supone una mínima injerencia en la vida privada de la persona, máxime aún si a través de la misma no se puede determinar aspectos como sus actividades, comportamientos o hábitos, en las diferentes esferas de desarrollo de su personalidad (Chanamé, 2015, pág. 203).

Por último, en cuanto al juicio de proporcionalidad en sentido estricto, la medida que se pretende ejecutar supone un sacrificio mínimo del derecho de la persona a la autodeterminación informativa, ya que, si bien esta información forma parte de su vida privada, frente a ella está un interés superior, el cual se manifiesta en el deber del Ministerio Público de investigar las conductas presuntamente delictivas, a través de una multiforme actividad investigativa, la cual se encuentra regulada legalmente y posee una fuerte relevancia del interés público (San Martín, 2020, pág. 122). Sobre este mismo eje, se puede llegar a la conclusión de que, con el solo requerimiento de información orientada a la identificación de titulares o terminales o dispositivos de conectividad, no se afecta el contenido esencial del derecho a la autodeterminación informativa, ya que dentro de su estructura, el Ministerio Público cuenta con lineamientos orientados a preservar la seguridad de la información así como su tratamiento, desde cláusulas de confidencialidad y de protección de datos personales, hasta directivas internas que rigen los distintos bancos de datos almacenados en el curso de las investigaciones, sobre las cuales, una vez finalizadas -dependiendo de su clasificación- el ciudadano tiene derecho a su acceso, rectificación, cancelación u oposición.

Por lo expuesto, se puede concluir que, conforme a la regulación actual, el Ministerio Público tiene todas las facultades para solicitar de manera directa a las empresas prestadoras de servicios de las telecomunicaciones, los datos que vinculan a un usuario específico con un número telefónico o con cualquier otro medio de comunicación, así como en sentido inverso, identifiquen algún número de teléfono o los datos identificativos de cualquier medio de comunicación con un determinado usuario. Ello, considerando que estos actos de investigación resultarían los más idóneos y proporcionados para lograr la individualización del investigado -finalidad perseguida, atendiendo a que se da mínimamente un sacrificio de derechos y/o intereses de los afectados, resultando superior el beneficio para el interés público.

En este contexto, se podría pensar que se trata de una medida irrelevante, ya que el Ministerio Público dentro de un proceso -usualmente- no solo requiere información sobre la identidad de un usuario del servicio de telecomunicaciones, sino que son necesarios más datos referidos al tráfico del servicio empleado. Sin embargo, se debe tener en cuenta que, en muchos casos, para culminar una investigación en curso no será necesario llegar a solicitar la intervención las telecomunicaciones; además, su utilidad también se vería reflejada para la identificación -al menos de manera indiciaria- del presunto autor del ilícito, con lo cual se cumpliría -desde el inicio- de manera irrestricta con el principio procesal de contradicción.

De esta manera, la aplicación de esta medida beneficiaría a la investigación de las modalidades delictivas que se sirven del anonimato, pudiendo el Ministerio Público hacer frente de manera inmediata y directa a delitos como el robo agravado (de celulares), receptación (de celulares), extorsión, fraude informático (phishing), el tráfico de drogas, la pornografía infantil, la suplantación de identidad, el acoso, el grooming, delitos contra la propiedad intelectual (distribución y venta), etc.

Como es de apreciar, la gama de delitos que pueden ser beneficiados en su investigación con esta medida son muy amplios, acortando de esta manera los

plazos excesivos, desde que la información era requerida por parte del Ministerio Público al Poder Judicial, pasando por la emisión de la resolución respectiva, hasta la respuesta de las empresas de telefonía.

A modo de colofón, se considera necesario hacer especial mención del Registro Nacional de Equipos Terminales Móviles para la Seguridad [RENTESEG]- Decreto Legislativo Nº 1338 y su reglamento. El RENTESEG se dio en el contexto de la prevención y lucha contra el hurto, robo y comercio ilegal de terminales móviles, estando su implementación y administración a cargo de OSIPTEL (Andina, 2020).

Este registro, de carácter permanente, está conformado por lo que la norma denomina lista blanca, lista negra e información de los eventos relacionados al uso de una línea (CDR). La lista blanca la integran: el registro de abonados proporcionado por las empresas operadoras, que contiene la información de los IMEI correspondientes a los equipos terminales móviles asociados al IMSI y/o MSISDN de las líneas activadas por las empresas operadoras a nivel nacional; la información de los equipos terminales móviles susceptibles de ser activados por estas empresas -equipos importados legalmente, ensamblados o fabricados en el país destinados para su comercialización en el mercado nacional o adquiridos en el exterior; los equipos terminales móviles recuperados de la Lista Negra; entre otros. Asimismo, es necesario precisar -para los fines de la presente investigación- que, respecto de los abonados que tienen un vínculo contractual con las empresas operadoras de servicio móvil, entre los datos mas importantes que almacena son: el código IMEI del equipo terminal móvil o número de serie electrónico que lo identifica; el código IMSI que activa el equipo terminal móvil; el número de servicio telefónico; tipo de abonado; modalidad contractual; nombre y apellidos completos del abonado o razón social; documento legal de identidad; fecha y hora de activación del servicio público móvil y estado del servicio.

En cuanto a la lista negra, son incorporados a esta los equipos móviles reportados como perdidos, hurtados, robados e inoperativos; los terminales móviles

no registrados en la lista blanca que sean detectados operando en la red del servicio público móvil; equipos cuyos códigos IMEI son detectados como alterados; entre otros.

Por último, también conforman el RENTESEG, la información de las empresas de telefonía contenida en sus CDR, esto es: el código IMEI, código IMSI y MSISDN de cada llamada saliente y entrante, mensaje de texto SMS, así como de la sesión de acceso a la red de datos; y la fecha, hora y código de la celda de la llamada saliente, de la llamada entrante, mensajes de texto SMS y de la sesión de acceso a la red de datos; debiendo aclarar que, según su normativa, no se almacena la identidad del abonado que realiza y recibe la llamada, o, el contenido de la llamada saliente y entrante, o, los mensajes de texto SMS, o, el contenido de la transferencia de datos realizada.

El RENTESEG, conforme el artículo 6 inciso 3 de su ley, y el artículo 18 inciso 3 de su reglamento, faculta al Ministerio del Interior, Ministerio Público y Poder Judicial a solicitar a OSIPTEL la información de los equipos terminales móviles contenida, tanto en la lista negra como en la lista blanca, en el ejercicio de sus funciones. Para ello, OSIPTEL ha implementado el Sistema de Gestión de Requerimientos de Información sobre IMEI [SIGREI], lo que permitiría a las entidades públicas acceder a la data y poder servirse de esta información.

Sobre este punto, es necesario precisar que, tanto la ley como el reglamento, hacen énfasis en que el acceso a la información de este registro se brinda a las entidades señaladas en el ejercicio de sus funciones de seguridad ciudadana, relacionadas a la sustracción y comercio ilegal de estos bienes, siendo esta su ratio legis. Sin embargo, llama la atención que el artículo 29 de su reglamento, brinde atribuciones a la Policía Nacional del Perú [PNP] para que esta, en el marco de la investigación de un delito, pueda solicitar a OSIPTEL la información contenida en el RENTESEG. Esta facultad, daría la posibilidad a la PNP a que, dentro de la investigación de cualquier delito, no solo los de naturaleza patrimonial, pueda solicitar de manera amplia la información contenida en el RENTESEG, no

limitándose a la lista blanca o negra, sino también a la información de los CDR de las empresas operadoras.

De esta manera, si se hace una interpretación amplia de los alcances y facultades que otorga el RENTESEG, se puede concluir que, si bien fue creado con el objetivo del fortalecimiento de la seguridad ciudadana en la lucha contra los delitos patrimoniales, específicamente aquellos vinculados con el hurto o robo de teléfonos celulares. Este, podría resultar una herramienta útil para la lucha contra cualquier tipo de delincuencia que se realice valiéndose de un terminal móvil.

Para finalizar, se debe precisar que, a la fecha de cierre de esta investigación, el RENTESEG se encuentra en proceso de implementación -estando en su tercera fase, habiendo celebrado convenios de interoperabilidad con el Ministerio del Interior para el uso del SIGREI, no habiéndose suscrito aún con el Ministerio Público. A pesar de ello, este registro se viene empleando por parte de la fiscalía, para determinar la identidad del agraviado en los delitos de receptación de equipos celulares, solicitando a OSIPTEL, mediante el código IMEI, la identidad del usuario que reportó el robo o hurto del terminal móvil; debiendo acotar que, debido a que el RENTESEG viene siendo implementado progresivamente, aún no ha sido posible que OSIPTEL se pronuncie sobre requerimientos en investigaciones que no están relacionadas con delitos patrimoniales, y sobre datos contenidos en la lista blanca, como:

- Cuando a partir de los datos de identificación del individuo se les solicita el número de la línea telefónica, el IMSI y el IMEI.
- Cuando a partir del IMSI de la línea telefónica se les solicita el número de la línea telefónica y los datos de identificación del titular.
- Cuando a partir del IMEI del terminal se les solicita el número de la línea telefónica y los datos de identificación del titular que consten en sus bases de datos.
- Cuando se les requiera cuál es la tarjeta SIM concreta con que está funcionando un determinado terminal de telefonía móvil o, en sentido

contrario, qué móvil concreto está siendo utilizado para el funcionamiento de una tarjeta SIM determinada.

Conclusiones

A continuación, se exponen las conclusiones a partir del análisis realizado ut supra:

1. La investigación de la criminalidad que se deriva del uso de las nuevas tecnologías hace necesario que se forjen nuevos criterios por parte de las diferentes entidades estatales, donde, si bien las nuevas tecnologías suponen una mayor exposición a riesgos, lo que motiva una mayor protección de los derechos fundamentales de las personas a la intimidad, vida privada o autodeterminación informativa; no debe suponer una tutela desproporcionada sobre estos derechos, que resulte en un actuar limitado por parte de los operadores de justicia.
2. A pesar de contar la normativa peruana con la Ley N° 30096 - Ley de Delitos Informáticos, esta se limita a regular aspectos del derecho penal sustantivo, dejando de lado el plano adjetivo, lo cual limita el accionar de los operadores de justicia en la investigación de diferentes delitos, sobre todo aquellos realizados a través de las TIC.
3. No existe ninguna limitación en la normativa peruana que impida al Ministerio Público a que, en el ejercicio de sus funciones constitucionalmente conferidas, requiera directamente a los operadores de telefonía a brindar datos de identificación de usuarios, terminales y dispositivos de conectividad.
4. Los datos que vinculan a un usuario con un número telefónico, el código IMEI de un equipo móvil y el código IMSI integrado en la tarjeta SIM, no están bajo el amparo del derecho al secreto y a la inviolabilidad de comunicaciones, por lo tanto, no sería necesario acudir al órgano jurisdiccional para requerir esta información.

5. La cesión de los datos señalados en el punto anterior por parte de las empresas de telefonía al Ministerio Público supone una injerencia mínima en los derechos fundamentales a la vida privada de las personas, frente al deber constitucional de este órgano en la lucha contra la criminalidad.
6. La Ley de Protección de Datos Personales peruana, no supone un impedimento a que las empresas proveedoras de servicios de comunicación, brinden los datos de identificación de usuarios, terminales y dispositivos de conectividad al Ministerio Público, siempre que se haga en el ejercicio de sus funciones, ya que para ello la norma se exime de sus alcances y dispensa de estas empresas de su deber de confidencialidad.
7. Se hace necesaria una norma de adecuación que permita, además de trasponer adecuadamente los alcances del Convenio sobre la Ciberdelincuencia, brindar herramientas procesales adecuadas a los operadores de justicia, teniendo en consideración que nuestro Código Procesal Penal no cuenta con medidas de investigación tecnológicas adecuadas para hacer frente al creciente índice de delitos cometidos mediante las nuevas tecnologías.

Glosario de Términos

Para fines de este apartado, se utilizará las definiciones plasmadas en el Reglamento del Decreto Legislativo Nº 1338:

- Abonado: Persona natural o jurídica que ha celebrado un contrato de prestación de servicio público móvil con alguna de las empresas operadoras de dichos servicios, independientemente de la modalidad de pago contratada.
- CDR: De las siglas en inglés Charging Data Records. Es un formato de recolección de información acerca de eventos relacionados al uso de una línea tales como tiempo de establecimiento de una llamada, duración de

la llamada, cantidad de datos transferidos, identificación del abonado llamante, entre otros.

- Empresa operadora: Persona jurídica que cuenta con un contrato de concesión, registro correspondiente o título habilitante para prestar servicios públicos móviles.
- Equipo terminal móvil: Dispositivo que posee un IMEI por medio del cual se accede a las redes de las empresas operadoras, para prestar servicios de telecomunicaciones de voz y/o datos.
- Equipo terminal móvil inoperativo: equipo terminal móvil que ha perdido de manera permanente alguna funcionalidad que no le permite operar en la red del servicio público móvil.
- Equipo terminal móvil sustraído: Equipo terminal móvil que ha sido hurtado o robado.
- IMEI alterado: IMEI que no corresponde a un código numérico válido y/o en el que no existe coincidencia con el originalmente establecido por su fabricante, es decir el IMEI físico no coincide con el IMEI lógico. Se considera IMEI alterado al código IMEI duplicado, clonado o inválido.
- IMSI: De las siglas en inglés International Mobile Subscriber Identity (Identificador Internacional de Suscriptor Móvil). Es el código de identificación internacional único para cada abonado del servicio público móvil, el cual se encuentra integrado a la SIM card, chip u otro equivalente, que permite su identificación a través de las redes de servicios móviles.
- MSISDN: De las siglas en inglés Mobile Station Integrated Services Digital Network. Es el número que identifica de forma única la suscripción en una red GSM o una red móvil UMTS.
- SIM card: Tarjeta del módulo de identificación del abonado (Subscriber Identity Module). Tarjeta inteligente que se inserta en un equipo terminal móvil, cuya función principal es la de habilitar el servicio del abonado o usuario, para su identificación en la red. Almacena de forma segura la clave de servicio del abonado o usuario, utilizada para identificarse ante

la red de la empresa operadora, de forma que sea posible cambiar la línea de un equipo terminal móvil a otro, mediante el cambio de dicha tarjeta. Se entenderá como SIM Card, USIM, Micro SIM, Nano SIM, Chip u otro equivalente.

- Servicio público móvil: Servicio de telefonía móvil, servicio móvil de canales múltiples de selección automática (troncalizado), servicio de comunicaciones personales (PCS) y otros que se definan posteriormente, de acuerdo a la normativa vigente.

Bibliografía

Doctrina

Agustina, J. R., Montiel Juan, I., & Gámez-Guadix, M. (2020). *Cibercriminología y victimología online.* Madrid: Síntesis.

Calvo López, D. (2017). Capacidades de actuación del Ministerio Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015: En especial la obtención de direcciones IP y numeraciones IMEI e IMSI (Apartados k) a m) del Art. 588 ter de la LECRIM). *Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid*, 1-30.

Castillo Cordova, L. (2005). El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional peruano. *Revista Peruana de Derecho Público, 6*(11), 127-151.

Chanamé Orbe, R. (2015). *La Constitución comentada* (Vol. I). Lima: Ediciones Legales.

Gaceta Jurídica. (2005). *La Constitución Comentada. Obra colectiva escrita por 117 autores destacados del País.* Lima.

López-Barajas Perea, I. (2017). Garantías constitucionales en la investigación tecnológica del delito: Previsión legal y calidad de la ley. *UNED. Revista de Derecho Político*(98), 91-119.

Marchal Escalona, N. (2017). *El derecho comparado en la docencia y la investigación.* Madrid: Dykinson.

Martínez Atienza, G. (2020). *Investigación tecnológicos en los Ciberdelitos.* Barcelona: Experiencia.

Miró Linares, F. (2011). La oportunidad en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología*(13-07), 07:1-07:55.

Miró Linares, F. (2012). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons.

Montoro Sánchez, J. A., & Sánchez Gómez, R. (2021). *Manual de derecho procesal penal para guardias civiles.* Madrid: Dykinson.

Mubarak Aguad, L. (2017). El Internet, el Bigdata y el tratamiento de datos personales. *Advocatus*(36), 205-223.

Rayón Ballesteros, M. C. (2019). Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015. *Anuario Jurídico y Económico Escurialense, LII*, 179-204.

Reátegui Sánchez, J. (2008). *El Control Constitucional en la etapa de calificación del Proceso Penal.* Lima: Palestra Editores.

Rivero Sánchez-Covisa, F. J. (2017). *Revisión del concepto constitucional del secreto de las comunicaciones.* Madrid: Dykinson.

Rubio Correa, M. A. (2013). *Los derechos fundamentales en la jurisprudencia del Tribunal Constitucional: análisis de los artículos 1, 2 y 3 de la Constitución.* Lima: Fondo editorial de la Pontificia Universidad Católica del Perú.

San Martín Castro, C. (2020). *Derecho Procesal Penal. Lecciones.* Lima: Instituto Peruano de Criminología y Ciencias Penales.

Valderrama Macera, D. J. (02 de agosto de 2021). *Medidas limitativas de derechos: medidas cautelares personales y reales (art. VI del título preliminar del CPP)*. Obtenido de LP: https://lpderecho.pe/medidas-limitativas-derechos-medidas-cautelares-personales-reales-articulo-vi-del-titulo-preliminar-cpp/

Varona Jiménez, A. (2020). Aspectos relevantes de la interceptación de las comunicaciones telefónicas en el proceso penal español. *Ius Inkarri. Revista de la Facultad de Derecho y Ciencia Política*(9), 159-172.

Jurisprudencia

Apelación, 726 (Audiencia Provincial - Cáceres, Sección 2ª 07 de septiembre de 2017).

Sentencia, EXP. N.° 2863-2002-AA/TC (Tribunal Constitucional 29 de enero de 2003).

Sentencia, 1417-2005-PA/TC (Tribunal Constitucional 12 de julio de 2005).

Sentencia, EXP. N.º 9426-2005-PHC/TC (Tribunal Constitucional 01 de diciembre de 2005).

Sentencia, EXP. N° 2235-2004-AA/TC (Tribunal Constitucional 18 de febrero de 2005).

Sentencia, 2596-2013-PHD/TC (Tribunal Constitucional 10 de noviembre de 2014).

Sentencia, Exp. N.° 04437-2012-PA/TC (Tribunal Constitucional 06 de agosto de 2014).

Legislación

Anteproyecto de ley orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, 97/2015 (JUSTICIA) (Consejo de Estado: Dictámenes 05 de marzo de 2015).

Anteproyecto de ley orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, 97/2015 (JUSTICIA) (Consejo de Estado: Dictámenes 05 de marzo de 2015).

Convenio sobre la Ciberdelincuencia [CC]. (23 de noviembre de 2001). *Serie de Tratados Europeos - N° 185*. Budapest.

Decreto Legislativo Nº 957 que aprueba el Código Procesal Penal (29 de julio de 2004).

Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana, N° 1338 (06 de enero de 2017).

Decreto Legislativo que aprueba la Ley Orgánica del Ministerio público, N° 052 (18 de marzo de 1981).

Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1338, Nº 007-2019-IN (04 de abril de 2019).

Decreto Supremo que aprueba el Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, N° 020-2007-MTC (Ministerio de Transportes y Comunicaciones).

Ley de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, N° 25 (18 de octubre de 2007).

Ley de procedimiento para adoptar medidas excepcionales de limitación de derechos en investigaciones preliminares, N° 27379 (21 de diciembre de 2000).

Ley de Protección de Datos Personales, N° 29733 (08 de enero de 2017).

Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, N° 13 (13 de octubre de 2015).

Ley Orgánica de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, N° 7 (26 de mayo de 2021).

Resolución de Consejo Directivo Nº 138-2012-CD-OSIPTEL (Organismo Supervisor de Inversión Privada en Telecomunicaciones 19 de setiembre de 2012).

Resolución Ministerial N° 111-2009-MTC/03 (Ministerio de Transportes y Comunicaciones 07 de febrero de 2009).

Informes

Agencia Española de Protección de Datos (2021). *Informe, N° 30*

Consejo Fiscal de la Fiscalía General del Estado. (2015). *Informe al Anteproyecto de ley orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas*.

Consejo General del Poder Judicial. (2015). *Informe al Anteproyecto de ley orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas.*

Oficina de análisis estratégico contra la criminalidad [OFAEC]. (2021). *Informe de analisis N° 04 - Ciberdelincuencia: Pautas para una investigación fiscal especializada.*

Unidad de Criminalidad Informática de la Fiscalía General del Estado [UNCRINFO]. (05 de marzo de 2019). Dictamen acerca del alcance de la reclamación de datos de identificación de titulares, terminales y/o dispositivos de conectividad prevista en el nuevo artículo 588 ter m de la Ley de Enjuiciamiento Criminal [UCRINFO].

Webgrafía

Andina. (18 de octubre de 2020). *Osipitel iniciará registro de equipos móviles a comercializarse en el país.* Obtenido de https://andina.pe/agencia/noticia-osipitel-inicia-registro-equipos-moviles-a-comercializarse-el-pais-818176.aspx

Defensoría del Pueblo. (2009). *Detenciones arbitrarias y responsabilidad del Estado. Estudio de casos.* Informe de Adjuntía N° 10-2009-DP/ADHPD, Lima. Obtenido de https://cdn.www.gob.pe/uploads/document/file/1191850/Informe-010-2009-DP-ADHPD20200803-1197146-hup6fh.pdf

El Peruano. (30 de diciembre de 2020). *Crean la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional y designan y nombran Fiscales en el Distrito Fiscal de Lima*. Recuperado el 26 de setiembre de 2021, de https://busquedas.elperuano.pe/normaslegales/crean-la-unidad-fiscal-especializada-en-ciberdelincuencia-de-resolucion-no-1503-2020-mp-fn-1916745-1/

El Peruano. (11 de junio de 2021). *Modifican la denominación de la Fiscalía Superior Especializada en Delitos de Ciberdelincuencia de Lima, en Fiscalía Superior de la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro y emiten otras disposiciones*. Recuperado el 26 de setiembre de 2021, de https://busquedas.elperuano.pe/normaslegales/modifican-la-denominacion-de-la-fiscalia-superior-especializ-resolucion-no-848-2021-mp-fn-1962667-1/

Iberley. (16 de agosto de 2019). *Identificación de usuarios, terminales y dispositivos de conectividad en el proceso penal*. Obtenido de https://www.iberley.es/temas/identificacion-usuarios-terminales-dispositivos-conectividad-proceso-penal-63150

OSIPTEL. (25 de enero de 2022). *Internet móvil: velocidad promedio en redes 4G se incrementó en todas las empresas operadoras al cierre del 2021.* Recuperado el 21 de abril de 2022, de https://www.osiptel.gob.pe/portal-del-usuario/noticias/internet-movil-velocidad-promedio-en-redes-4g-se-incremento-en-todas-las-empresas-operadoras-al-cierre-del-2021/