UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

Facultad Derecho y Ciencias Políticas

Carrera Profesional de Derecho

TESIS

PARA OBTENER EL TÍTULO DE ABOGADO

TÍTULO DE LA TESIS

VULNERACIÓN DEL DERECHO FUNDAMENTAL A LA INTIMIDAD CON LA IMPLEMENTACIÓN DEL DECRETO LEGISLATIVO N° 1182, SOBRE GEOLOCALIZACIÓN EN LOS DELITOS DE CRIMEN ORGANIZADO, SIN AUTORIZACIÓN JUDICIAL POR LA DIVINCRI EN EL DISTRITO DE CAJAMARCA - 2019.

Tesis presentada en cumplimiento parcial de los requerimientos para optar el Título Profesional de abogado.

PRESENTADO POR:

Bach. Guido Antuan Marín Vásquez

Bach. García Ugaz Joel Danny

ASESOR: Mg. Quevedo Miranda Augusto Rolando

Cajamarca- Perú

Febrero – 2021

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

Facultad Derecho y Ciencias Políticas

Carrera Profesional de Derecho.

TESIS

PARA OBTENER EL TÍTULO DE ABOGADO

TÍTULO DE LA TESIS

VULNERACIÓN DEL DERECHO FUNDAMENTAL A LA INTIMIDAD CON LA IMPLEMENTACIÓN DEL DECRETO LEGISLATIVO N° 1182, SOBRE GEOLOCALIZACIÓN EN LOS DELITOS DE CRIMEN ORGANIZADO, SIN AUTORIZACIÓN JUDICIAL POR LA DIVINCRI EN EL DISTRITO DE CAJAMARCA - 2019.

Tesis presentada en cumplimiento de los requisitos para optar el Título Profesional de Licenciados en Derecho y Ciencia Política.

PRESENTADO POR:

Bach. Guido Antuan Marín Vásquez
Bach. García Ugaz Joel Danny

ASESOR: Mg. Quevedo Miranda Augusto Rolando

Cajamarca- Perú

Febrero - 2021

UNIVERSIDAD PRIVADA ANTONIO GUILLERMO URRELO

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA PROFESIONAL DE DERECHO

APROBACIÓN DE TESIS PARA OPTAR TÍTULO PROFESIONAL

TÍTULO DE LA TESIS

VULNERACIÓN DEL DERECHO FUNDAMENTAL A LA INTIMIDAD CON LA IMPLEMENTACIÓN DEL DECRETO LEGISLATIVO N° 1182, SOBRE GEOLOCALIZACIÓN EN LOS DELITOS DE CRIMEN ORGANIZADO, SIN AUTORIZACIÓN JUDICIAL POR LA DIVINCRI EN EL DISTRITO DE CAJAMARCA - 2019.

Presidente **:** Mg. Gutiérrez Portal Edgar Elí

Secretario **:** Mg. Vargas Carrera Juan

Asesor **:** Mg. Quevedo Miranda Augusto Rolando

A:

La presente tesis se la dedicamos a Dios, quién nos guio por el sendero de la Luz, y por el largo camino de superación, dándonos fuerza y coraje para enfrentarnos a las adversidades y seguir adelante y caer.

A cada una de nuestras familias, porque con su apoyo y comprensión hemos ido día a día enfrentando los obstáculos que se nos presentó durante la elaboración de la presente.

Por último, agradecer al Brigadier Calderón Movallón, encargado del área de Geolocalización de la División de Investigación de Criminalística (DIVINCRI) del distrito de Cajamarca, quien proporcionó la información necesaria para el desarrollo de nuestra tesis, puesto que sin su apoyo no hubieses podido realizarla.

Los autores.

TABLA DE CONTENIDOS

SIGLAS Y ABREVIATURAS.

CAJ **:** Cajamarca

D.L. **:** Decreto Legislativo.

DAO O CAD : Diseño asistido por Ordenador.

DEPINCRI **:** Departamento de Investigación Criminal

DIRINCRI **:** Dirección de Investigación Criminal

DIVINCRI **:** División de Investigación Criminal

DIVICAJ **:** División de investigación de Cajamarca.

FRENPOL **:** Frente Policial.

GPS **:** Sistema de Posicionamiento Global.

GSM : Global System for mobile communications (Sistema globar para las comunicaciones móviles.

ICT **:** Information and communications technology.

IT : Information techonology.

NCPP **:** Nuevo Código Procesal Penal.

NTICS : Nuevas Tecnologías de la información y la comunicación.

ONGD **:** Organismos no gubernamentales de desarrollo

PNP **:** Policía Nacional del Perú

SCG	**:** Sistema De Control Gubernamental
SIG.	: Sistema Informático geográfico.
TI.	: Tecnologías de la Información.
TICs.	**:** Tecnologías de la información y comunicaciones.
TIGs.	**:** Tecnologías de la información geográfica.

GLOSARIO DE TÉRMINOS.

- **Amenazas.** Delito consistente en intimidar a alguien con el anuncio de la provocación de un mal grave para él o su familia. (Asociación de Académias de la Lengua Española., 2009)

- **Comisión de delito.** Tiempo en que ha de considerarse el hecho delictivo, que generalmente determina cuál es la ley aplicable a los hechos. (Asociación de academías de la lengua española, 2015)

- **Conectividad.** Es la capacidad de un dispositivo (ordenador personal, periférico, PDA, móvil, robot, electrodoméstico, automóvil, etc.) de conectarse y comunicarse con otro, con el fin de intercambiar información o establecer una conexión directa a base de información digital. (Wikipedia., 2020)

- **Crimen organizado.** Son grupos de personas que se dedican a traficar drogas, personas, cometer secuestros, asesinatos, entre otros delitos. También llamado delincuencia organizada, en estos grupos existe cierta jerarquía, roles y funciones. (Iniseg, 2019)

- **Cuasiflagrancia.** Se considera en situación de cuasiflagrancia la persona sorprendida con objetos, instrumentos o huellas, de los cuales aparezcan fundadamente que ha cometido un hecho punible o participado en él; o cuando es perseguida por la autoridad; o cuando por voces de auxilio se pide su captura. (Pasión por el Derecho, 2020)

- **Datos.** Información concreta sobre hechos, elementos, etc., que permite estudiarlos, analizarlos o conocerlos.

- **Delincuencia común.** La delincuencia común es aquella que opera sin estructuras organizativas, sino mediante individuos o grupos de individuos que cometen delitos

menores o graves, principalmente con el objetivo de obtener dinero o artículos de valor. No son delincuentes especializados. (Significados, 2017)

- **Departamento de Investigación Criminal (DEPINCRI). -** Se encarga de investigar las denuncias de todo tipo de delitos en forma directa o mediante las derivaciones de otras dependencias policiales. Las DEPINCRI operan en el interior del país. (Ministerio de Cultura, 2002)

- **Derecho a la intimidad.** Consiste en la defensa de la persona en su totalidad a través de un muro que prohíbe publicar o dar a conocer datos sobre temas como la religión, la política o la vida íntima. (Wikipedia, 2017)

- **Derecho a la privacidad.** Aquel derecho humano por virtud del cual la persona, llámese física o moral, tiene la facultad o el poder de excluir o negar a las demás personas, del conocimiento de su vida personal, además de determinar en qué medida o grado esas dimensiones de la vida personal pueden ser legítimamente comunicados a otros.

- **Derecho al secreto de las comunicaciones.** Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. (Abad, S, 2009)

- **Derecho comparado.** Suele ser calificado como una disciplina o método de estudio del derecho que se basa en la comparación de las distintas soluciones que ofrecen los diversos ordenamientos jurídicos para los mismos casos planteados

- **Derechos fundamentales.** Son todos aquellos atribuibles a todas las personas sin excepción, y que se consideran como un listado de reglas básicas y preeminentes en el ordenamiento jurídico. Estos son notoriamente diferentes al resto de derechos porque son inalienables (se adquieren desde el nacimiento) y no pueden ser objeto de transacción o

intercambio en el contrato de trabajo, aunque pueden sufrir alguna modulación por lo que el trabajador está subordinado y tiene dependencia del empresario. Algunos de estos derechos se rigen no solamente desde el inicio de la relación laboral, sino también en los procesos de selección y claro está, en el despido también.

- **Dirección de Investigación Criminal (DIRINCRI).-** Su función es de investigar, denunciar y combatir la delincuencia común, el crimen organizado y otros hechos trascendentes en el ámbito nacional y la delincuencia internacional, en los campos de los delitos Contra la Vida, el Cuerpo y la Salud, el Patrimonio, la Libertad, la Familia, contra la Confianza y la Buena Fe en los Negocios, contra los Derechos Intelectuales, contra el Orden Financiero y Monetario, contra el Orden Migratorio, contra la Fe Pública, contra la Humanidad, Usurpación de Autoridad y otros: Así como la búsqueda de personas desaparecidas, aprehendiendo los indicios, evidencias y pruebas; identificando y capturando a los autores y partícipes, con la finalidad de ponerlos a disposición de la autoridad competente; asimismo, dar cumplimiento a la ejecución, difusión y registro de órdenes judiciales, capturas, notificaciones, conducciones de grado o fuerza, requisitorias, impedimento de salida y/o ingreso al país, oposición o suspensión de viaje de menores al exterior y otros dispuestos por la autoridad competente; igualmente, ejecutar los mandatos del Ministerio Público, relacionados con la investigación de delitos, así como prestarles el asesoramiento y apoyo necesario para el mejor cumplimiento de sus funciones.

- **Dispositivo electrónico.** Consiste en una combinación de componentes electrónicos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas. los aparatos electrónicos a diferencia de los eléctricos utilizan la electricidad para el almacenamiento, transporte o transformación de información. (Wikipedia, 2017)

- **División de investigación criminal (DIVINCRI). -** Se encarga de investigar, denunciar la comisión de los Delitos Contra la Vida y el Cuerpo y la Salud, contra el patrimonio, contra la Libertad y la Familia, sobre hechos denunciados en forma directa o derivados de las comisarias, captura de presuntos autores de delitos. En la actualidad está dividida por las DIVINCRI Norte, Sur, Este y Oeste; que operan en Lima metropolitana.

- **División de Investigación Criminal y apoyo a la Justicia (DIVICAJ). -** Jefatura que se encarga de investigar las denuncias específicas de delincuencia común y crimen organizado en sus diferentes modalidades.

- **Fiscalía de la Nación.** Es el órgano de la alta dirección. El Fiscal de la Nación preside el Ministerio Público y junto con los Fiscales Supremos Titulares constituyen la Junta de Fiscales Supremos. Este órgano es el que elige al máximo representante de la Fiscalía de la Nación. (Ministerio Público - Fiscalía de la Nación, s.f.)

- **Flagrancia delictiva.** Existe flagrancia cuando la realización del hecho punible es actual y, en esa circunstancia, el autor es descubierto, o cuando es perseguido y capturado inmediatamente de haber realizado el acto punible o cuando es sorprendido con objetos o huellas que revelan que acaba de ejecutarlo.

- **Geolocalización.** Capacidad para obtener la ubicación geográfica real de un objeto, como un radar, un teléfono móvil o un ordenador conectado a Internet.

- **Informes Policiales. -** El Informes Policiales es un documento oficial que puede dar paso a una investigación sobre la denuncia y permitirá a la policía tomar determinadas acciones. El informe policial permite a la Policía Nacional informarse del delito denunciado.

- **Interceptación.** La interceptación ocurre cuando un tercero escucha una conversación telefónica privada, pero también puede hacerse a comunicaciones por correo electrónico o a mensajes de texto enviados por dispositivos móviles o por computadores conectados a redes Wi -Fi. (Salazar, S, 2020)

- **Investigación.** Es una actividad orientada a la obtención de nuevos conocimientos o, ampliar estos su aplicación para la solución a problemas o interrogantes de carácter científico.

- **Policía nacional del Perú.** La Policía Nacional del Perú es una institución del Estado que tiene por misión garantizar, mantener y restablecer el orden interno, prestar protección y ayuda a las personas y a la comunidad, garantizar el cumplimiento de las leyes y la seguridad del patrimonio público y privado, prevenir, investigar y combatir la delincuencia; vigilar y controlar las fronteras; con el propósito de defender a la sociedad y a las personas, a fin de permitir su pleno desarrollo, en el marco de una cultura de paz. (Gob. pe, s.f.)

- **Protección de datos.** Para lo cual prescribe que el tratamiento de sus datos personales sea proporcional y seguro, de acuerdo con finalidades consentidas por tales personas o habilitadas por ley, previniendo así que tales datos sean objeto de tráfico y/o uso ilícito.

- **Región policial:** son órganos que ejercen las funciones, atribuciones y competencias de la Policía Nacional del Perú en un determinado espacio geográfico del territorio nacional. Están a cargo de Oficiales Generales o Coroneles de la Policía Nacional del Perú en situación de actividad.

- **Sistema de información geográfica.** es un marco de trabajo para reunir, gestionar y analizar datos. Arraigado en la ciencia geográfica, SIG integra diversos tipos de datos.

Analiza la ubicación espacial y organiza capas de información para su visualización, utilizando mapas y escenas 3D. (Wikipedia, s.f.)

- **Tecnología de la información geográfica.** Las Tecnologías de la Información Geográfica (TIG), concretamente los Sistemas de Información Geográfica, la Teledetección, la Cartografía digital, los GPS o la Fotogrametría constituyen una nueva ciencia en creciente expansión, debido a su variabilidad en su aplicación con ámbitos tan distintos como el medio ambiente y los recursos naturales, la demografía, la gestión de servicios públicos, el urbanismo, la ordenación del territorio, la planificación del transporte, el geomarketing, etc. Los Objetivos que se han planteado con la publicación de este libro son dar a conocer el potencial y las funcionalidades de estas tecnologías con la exposición de casos prácticos de usos en la Administración, la empresa privada, la Universidad o la investigación aplicada. (Masot, N, 2019)

- **Tecnología de la información y comunicaciones.** Las tecnologías de la información y comunicación (TIC) son el resultado de poner en interacción la informática y las telecomunicaciones. Todo, con el fin de mejorar el procesamiento, almacenamiento y transmisión de la información. (Bernejo, D, 2021)

- **Vulneración de Derechos.** Trasgresión a los derechos; cualquier vulneración de derechos es grave, por lo que los Estados deben realizar todas las acciones destinadas a prevenir estos hechos y a entregar mecanismos de restitución de derechos una vez ya vulnerados.

INDICE TABLAS Y GRÁFICOS

TABLAS

GRÁFICOS

RESUMEN.

Acceder a los metadatos de geolocalización de los dispositivos móviles de cualquier ciudadano cuando se encuentren frente a un delito flagrante, este sea castigado con una pena superior a los 4 años y el acceso sea necesario para realizar la investigación. Sin que este acceso no requiera mandato judicial previo y se regulariza ante el Juez con posterioridad. Acarrea una serie de consecuencias negativas. La presente investigación tiene como **objetivo general:** Determinar cómo vulnera el derecho fundamental de la intimidad con la implementación del Decreto Legislativo N° 1182, referido a la Ley de Geolocalización, en los delitos de Crimen Organizado sin autorización judicial, por la División de Investigación Criminal. La cual tiene por finalidad es analizar y explicar el Decreto Legislativo N° 1182, referido a la geolocalización para determinar las implicancias negativas que dan origen a la vulneración del derecho fundamental de intimidad. Surgiendo la interrogante ¿Cómo se vulnera el derecho fundamental de la intimidad con la implementación del Decreto Legislativo N° 1182, sobre geolocalización, en los delitos de crimen organizado sin autorización judicial por la DIVINCRI en el Distrito de Cajamarca – 2019?

Dicha investigación parte de una **metodología** de tipo Aplicada de diseño descriptivo – explicativo, no experimental de corte transversal, de enfoque cualitativa y cuantitativa, atendiendo a las variables geolocalización; derechos fundamentales y, derecho comparado. De los **resultados** obtenidos se puede apreciar que con la implementación del Decreto Legislativo N° 1182, sobre geolocalización, en los delitos de crimen organizado sin autorización judicial por la DIVINCRI en el Distrito de Cajamarca: Se vulnera el derecho fundamental de la intimidad. Los procedimientos del decreto del decreto legislativo 1182 no se cumplen de manera adecuada, siendo estos ineficientes. La legislación comparada regula

el acto de investigación de geolocalización en la norma penal y norma especial, respaldando la facultad del efectivo PNP de hacer uso de la geolocalización sin autorización judicial.

Finalmente se **concluye** que, en el Distrito de Cajamarca, se emplea la geolocalización sin autorización judicial, vulnerando el derecho fundamental de la intimidad, y en algunos casos resulta siendo ineficiente en la investigación dentro los delitos de Crimen Organizado.

Palabras Claves: Geolocalización. Derechos Fundamentales, Metadatos, ubicación, vulneración.

Línea de Investigación: Investigación Jurídica. Derecho Constitucional.

ABSTRACK.

Access the geolocation metadata of any citizen's mobile devices when faced with a flagrant crime, it is punishable by more than 4 years and access is necessary to carry out the investigation. This access does not require prior judicial mandate and is subsequently regulated before the Judge. It has a number of negative consequences. The general objective of this investigation is to determine how the fundamental right of privacy violates the implementation of Legislative Decree No. 1182, referring to the Geocalization Act, in crimes of organized crime without judicial authorization, by the Criminal Investigation Division. The purpose of the report is to analyze and explain Legislative Decree No. 1182 on geolocation in order to determine the negative implications that give rise to the violation of the fundamental right of privacy. The question arises: How is the fundamental right of privacy violated with the implementation of Legislative Decree No. 1182 on geolocation in crimes organized without judicial authorization by the DIVINCRI in the District of Cajamarca – 2019?

This research is based on a methodology of applied type of descriptive – explanatory, non-experimental cross-sectional design, of qualitative and quantitative approach, taking into account the variables geolocation; fundamental rights and, comparative law. From the results obtained, it can be seen that with the implementation of Legislative Decree No. 1182 on geolocation, in crimes of organized crime without judicial authorization by the DIVINCRI in the District of Cajamarca: The fundamental right of privacy is violated. The procedures of the decree of legislative decree 1182 are not adequately complied with, these being inefficient. The comparative legislation regulates the act of investigation of geolocation in the penal norm and special norm, supporting the power of the NPP cash to make use of geolocation without judicial authorization.

Finally, it is concluded that, in the District of Cajamarca, geolocation is used without judicial authorization, violating the fundamental right of privacy, and in some cases it becomes inefficient in the investigation into organized crime crimes.

Keywords: Geolocation. Fundamental rights, metadata, location, violation.

CAPÍTULO I: INTRODUCCIÓN.

1.1.Planteamiento del Problema.

1.1.1. Descripción de la Realidad Problemática.

La lucha contra la delincuencia es una tarea en la que la sociedad está llamada a jugar un rol importante como colaboradora y facilitadora. Sin embargo, este rol no puede significar despojar a los ciudadanos de derechos fundamentales y vulnerar las garantías constitucionales. Las normas aprobadas por el Poder Ejecutivo a través del Decreto Legislativo N° 1182; han excedido ese equilibrio y pueden hacer más daño del que pretenden evitar.

El Decreto Legislativo N° 1182, determina incorrectamente que la información sobre la ubicación de un usuario, obtenida mediante la geolocalización de su teléfono móvil, no forma parte del contenido constitucionalmente protegido del secreto y la inviolabilidad de las comunicaciones.

Siguiendo este razonamiento, la norma propone que el acceso a dicha información puede ser ejecutado por la policía sin la necesidad de contar con una autorización judicial previa, estableciendo un mecanismo de aprobación judicial posterior para legitimar esta acción. *El artículo 10 de la Constitución contradice esto, al establecer que cualquier procedimiento que involucre el acceso a esta información por parte de un tercero debe de ser autorizado y motivado por un juez.*

Además de la inconstitucionalidad de sus medidas, el Decreto Legislativo N° 1182 interfiere también con la implementación del Nuevo Código Procesal Penal en la medida que resta atribuciones al Ministerio Público de forma ilegítima e invalida de

facto normas penales que ya disponían cómo debía ser la solicitud y el acceso a los datos de geolocalización. Todas estas medidas buscan ampararse en la interpretación de que la policía puede actuar de esta manera cuando esté frente a un delito flagrante. Por supuesto, esta interpretación está llena de deficiencias y no tiene sustento en la jurisprudencia nacional.

El Decreto Legislativo N° 1182, también obliga a las empresas de telecomunicaciones a registrar y conservar los datos relacionados con las comunicaciones de sus usuarios, incluyendo registros de llamadas, navegación por Internet y ubicación geográfica.

De esta forma, se ordena crear gigantescas bases de datos privadas que estarán a disposición del escrutinio policial durante el plazo de tres (3) años. Esto no es más que la legalización de la vigilancia masiva e indiscriminada, cuya implementación en estas condiciones no resulta necesaria, idónea ni proporcional a los fines que persigue.

En otros países existen actualmente normativas similares que ya fueron derogadas, archivadas o enfrentan procesos para que se evalúe su constitucionalidad. En atención a todo lo expuesto, es necesario derogar parcialmente el referido Decreto Legislativo en los extremos en los que:

- Permite el acceso sin autorización judicial de la Policía a la ubicación de cualquier usuario de dispositivos móviles, y,

- Ordena a las empresas de telecomunicaciones a conservar los datos derivados de las telecomunicaciones de sus usuarios por un período de tres años.

Así las implicancias negativas de la aplicación de una norma de esta naturaleza pues entre sus mecanismos de funcionamiento se contemplan el acceso y uso de los

datos arriba referidos sin un mandato judicial previo y la retención de la totalidad de datos derivados de las telecomunicaciones por un largo período de tiempo. Por lo que se busca identificar los puntos más controvertidos de este decreto legislativo y ofrecer el sustento legal suficiente para su derogación.

1.2. Planteamiento del Problema.

¿Cómo se vulnera el derecho fundamental de la intimidad con la implementación del Decreto Legislativo N° 1182, sobre geolocalización, en los delitos de crimen organizado sin autorización judicial por la DIVINCRI en el Distrito de Cajamarca – 2019?

1.3. Objetivos.

1.3.1.1. Objetivo General.

Determinar cómo se vulnera el derecho fundamental de la intimidad con la implementación del Decreto Legislativo N° 1182, referido a la Ley de Geolocalización, en los delitos de Crimen Organizado sin autorización judicial, por la División de Investigación Criminal por la DIVINCRI en el Distrito de Cajamarca.

1.3.1.2. Objetivos Específicos.

- Desarrollar dogmáticamente temas referentes a geolocalización.
- Analizar los informes respecto de las denuncias de las víctimas por delitos de crimen organizado, registrado por el FRENPOL-CAJ-DIVINCRI-DEPINCRI-ARESE-SCG, durante el año 2019 en el Distrito de Cajamarca.

- Examinar los procedimientos que establece 1182, sobre su eficiencia y eficacia en el contexto peruano y el derecho comparado.

1.4. Justificación e importancia.

Para definir, comprender y hacer frente sobre la problemática que surge de la incorporación del Decreto Legislativo N° 1182, que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado, a través del uso de tecnología de la información y comunicaciones por parte de la PNP.

En el Decreto Legislativo se visualiza la potestad que se le otorga a la Policía de acceder a los metadatos de geolocalización de los dispositivos móviles de cualquier individuo.

Ahora la presente norma determina que: ***se utilizará cuando cualquier ciudadano se encuentre frente a un delito flagrante; sea castigado con una pena superior a los 4 años y que el acceso sea necesario para realizar la investigación.*** Este acceso no requiere mandato judicial previo y se regulariza ante el Juez con posterioridad.

En muchas formas, el acceso a datos y metadatos de geolocalización como política pública representa en sí misma una amenaza a la privacidad de todos los ciudadanos. Ahora, tales efectos negativos pueden ser disminuidos por diferentes medidas, desde el respeto a los derechos fundamentales (Derecho al secreto de las comunicaciones y el Derecho a la Intimidad); hasta límites al acceso como las condiciones que lo habilitan; el tiempo máximo; quienes puede acceder; entre otras. En nuestro país, los problemas asociados a esta política pública son:

- Afectan el derecho a la intimidad de todas las personas, aun las que no son

investigadas por la comisión de delitos, pero que mantienen comunicación con personas investigadas. Pese a que las leyes actuales ordenan que las comunicaciones o las grabaciones que no sean necesarias para la investigación deben ser eliminadas, existen múltiples agentes a cargo de esta información, lo que aumenta el riesgo de fugas y la revelación por parte de terceros.

- Afectan el derecho a las personas a que sus metadatos (como el de geolocalización) sean igual de protegidos que sus comunicaciones pues las normas actuales permiten el acceso a las mismas sin un mandato judicial, lo que disminuye las garantías de las personas que son investigadas usando esta medida. Además, como el protocolo de uso es secreto y los investigados nunca son informados de la aplicación de esta medida, las situaciones de uso abusivo o desproporcionado no se pueden conocer generando impunidad en quienes lo utilizan indebidamente.

- Afectan la economía de los usuarios finales, pues los costos que asumen las compañías de telecomunicaciones al recolectar estos datos y metadatos y hacerlos disponibles de forma permanente a las autoridades se refleja finalmente en la contraprestación que estos tienen que pagar para acceder a los servicios de telecomunicaciones.

Su importancia como aporte científico dentro de la investigación radica desde el punto de vista:

- *Teórica.* - Al profundizar en uno o varios enfoques teóricos que tratan el problema que se detalla de manera que se espera avanzar en el conocimiento.

- *Práctica.* - La cuál, está orientada a perfeccionar el trabajo de manera que indica la aplicabilidad de la investigación, su proyección de la sociedad, quienes se benefician

de ésta, ya sea un grupo social o una organización.

La investigación tiene justificación práctica cuando su desarrollo ayuda resolver un problema o por lo menos pone estrategias que, de aplicarlas contribuirían a resolverlo, vale decir, explicar por qué es conveniente es llevar a cabo la investigación y cuáles son los beneficios que se derivaran de ella.

- *Metodológica.* Dicha investigación implica un proceso de varias fases: métodos, procedimiento y técnicas e instrumentos empleados durante la investigación a fin de demostrar su validez y confiabilidad que sirva para otras investigaciones.

CAPITULO II: MARCO TEÓRICO.

2.1. Antecedentes Teóricos.

2.1.1. Internacionales.

Gonzales, J. (2013). En su artículo: *Derechos Fundamentales Afectados por la Geolocalización*. Hace referencia a:

> Precisar la legalidad o ilegalidad de la Geolocalización, en relación con los Derechos Fundamentales contenidos en los artículos 18.1 y 18.3 de la Constitución española. En la esfera de los Derechos Fundamentales afectados, se deduce que existe un conflicto de intereses entre los distintos Derechos y distintos sujetos que son objeto de estudio. En conflicto existe, porque las autoridades deben proteger la seguridad de los ciudadanos; los proveedores de servicio, porque la ley les obliga a guardar los datos durante un tiempo y los ciudadanos, desean que, en ningún caso, se intervenga el contenido de las comunicaciones. (González. J, 2013)

Flores, M. (2016). En su artículo: *La Geolocalización y el Derecho a la Privacidad. Análisis de la Acción de la Inconstitucionalidad 32/2012.* Hace referencia a:

> El Pleno de la Suprema corte de Justicia de la Nación al resolver la acción de inconstitucionalidad 32/2012 determinó que en la geolocalización existe una búsqueda que se refiere a los equipos de comunicación móvil y no a personas, por lo tanto, de ningún modo constituye una restricción a la vida privada de las personas, ya que no se encuentra dirigida a buscar personas sino un instrumento del delito. Las normas que prevén la geolocalización resultan válidas para atender a los criterios de fin legítimo, idoneidad, necesidad y proporcionalidad. Es así, que alguna información privada pudiera ser revelada con el uso de esta medida, la misma resulta justificable por los fines constitucionales que persigue, a saber: la seguridad de las víctimas y la persecución, y sanción de ilícitos penales. En consecuencia, el tribunal fijó límites a la atribución del Ministerio Público, ya que deberán dejar constancia de dicha solicitud en el expediente de la investigación respectiva, y motivar el requerimiento sólo en casos de extrema urgencia, es decir: Cuando esté en riesgo la vida o la integridad física de una persona; Cuando pueda ocultarse o desaparecer el objeto de la investigación. Y Siempre que se trate de delitos como secuestro, amenazas, crimen organizado, delitos contra la salud o

extorsión. (Flores. M, 2016).

Cabellos, L. (2017). En su tesis: *Datos de Geolocalización como medida de Investigación. Avances en el Sistema Jurídico Procesal Penal*. Determina que:

> Las nuevas tecnologías y el avance de las comunicaciones han variado la forma de delinquir y de investigar al delincuente. Los datos de geolocalización han sido tratados de forma tangencial aprovechando regulaciones de otras materias, y de manera insuficiente. Esto supone que se ha infravalorado su función como medida de investigación y su naturaleza como fuente de prueba, sin que parezca haberse percatado de la real trascendencia de estos datos, ya que incluso pueden afectar un derecho fundamental como el derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución española). (Cabellos. L, 2017)

Fernández del Campo, I. (2015). *Los Servicios de Geolocalización y el Derecho a la Protección de Datos Personales.* En su investigación hace referencia a:

> Los servicios de geolocalización están en auge como consecuencia de la tecnología. Si bien las posibilidades pueden resultar útiles merecen las más cautas aproximaciones, puesto que al mismo tiempo presentan riesgo de tratamientos indebidos o indeseados. Los datos de geolocalización revisten un valor considerable por permitir, mediante la inducción y cruzado con otros datos, la identificación de un individuo y la elaboración de un perfil del mismo. Un mal tratamiento, el cual incluiría la deficiente adopción de medidas de seguridad, puede brindar información de interés económico y personal a terceros que, por razones de seguridad, empresariales y personales, su titular puede preferir mantener fuera de la mirada ajena. Ante tratamientos indebidos o deficientes de los datos recogidos con aplicaciones de geolocalización la responsabilidad recae sobre el responsable del tratamiento. El resto de los sujetos solo será responsable en la medida que excedan sus funciones de intermediarios técnicos o confluyan en ellos su posición de intermediario con la de titular de la aplicación. (Fernández del Campo, I, 2015)

Salvador, E. (2018). En su tesis: *La problemática de la Protección de Datos Personales y la Geolocalización.* En su investigación llego a concluir que:

> El uso de este mecanismo implica un riesgo cuando se utilizan sin discriminar los permisos a los que consentimos cuando accedemos a utilizar la tecnología; generando vulneraciones a derecho a la protección de datos de los sujetos, por la información obtenida como: Género, edad, número telefónico, localización, etc. Existe la necesidad de

crear una norma específica sobre la protección de datos personales y esta normativa debe reconocer la geolocalización como un dato personal. (Salvador. E, 2018).

Martínez, R. (2016). En su artículo: *Geolocalización: Entre el Bien Común y el Derecho a la Privacidad.* En su investigación hace referencia a que:

> La geolocalización, puede ser una herramienta de suma utilidad en la investigación y persecución de los delitos. Asimismo, el uso de la geolocalización debe ser ponderada, considerando la colisión que se podría generar entre la seguridad, integridad física y el bien común, en relación con el derecho a la privacidad y la protección de los datos personales. Arribando que, para que el uso de la geolocalización sea parte de las políticas gubernamentales para la prevención y persecución del delito no vulneren la vida privada y los datos personales deben: Generar una regulación clara, que establezca de forma precisa en qué casos se puede utilizar la geolocalización; La normativa debe instituir que para el uso de la geolocalización debe mediar mandato judicial, para respetar el principio de seguridad jurídica contenido en el artículo 16 constitucional; - Hacer un análisis ponderado de los supuestos hipotéticos, que pudieran dar como resultado un Manual de Procedimientos para el uso de la geolocalización; Establecer canales de comunicación entre el gobierno y los concesionarios de telecomunicaciones para seguir procedimientos estandarizados en los casos que se les requiera a estos últimos la geolocalización de personas sujetas a investigaciones delictivas. (Martínez R, 2016)

2.1.2. Nacionales.

Yupanqui, C. (2015). En su Tesis: *Impacto del Decreto Legislativo N° 1182 en el Contenido esencial de los Derechos a la Información y libertad de expresión*. En su investigación se determina que:

> La interpretación sobre si la nueva norma permite al efectivo policial saber dónde está cualquier persona sin orden Judicial. El autor manifiesta que antes de la promulgación de la presente ley era necesario la solicitud de un Fiscal y la autorización de un Juez para acceder a estos datos. Asimismo, indica que el estado no ha acreditado la necesidad de vulnerar derechos Fundamentales siendo esta una violación grave a la Constitución. (Yupanqui. C, 2015).

Neciosup, S. (2017). En su tesis: *Afectación de los Derechos Constitucionales por la Aplicación del Decreto Legislativo N°1182 referido a la Ley de Geolocalización en*

su Implicancia en la Ciudad de Chiclayo. En su investigación hace referencia que:

> La afectación de derechos constitucionales por la aplicación del Decreto Legislativo N°1182 se ve afectado por Empirismos Normativos y Discrepancias Teóricas debido a que conocen el planteamiento teórico como son: Derecho a la Intimidad y Derecho a la Privacidad de las personas; pero no lo consideran o no lo toman en cuenta en la Disposición Complementaria Final Segunda del Decreto Legislativo N° 1182, referido a la retención de datos; la cual no cumple con lo normado en las leyes peruanas, vulnerando u afectando los Derechos Constitucionales de los ciudadanos; pues no existe claridad con respecto a los límites y controles de seguridad. (Neciosup. S, 2017).

Elías, R. (2016). En su artículo: *Decreto Legislativo 1182, Geolocalización y Proceso Penal. Sacrificio de Garantías en favor de una supuesta Eficacia Investigativa.* Aquí hace referencia a que:

> Se requiere una urgente modificación del Decreto Legislativo 1182 porque pone en riesgo la seguridad de todos los ciudadanos. Así, al encontrarnos en un Estado Constitucional de Derecho, exigimos que sea la autoridad judicial quien previamente autorice el acceso a información sensible como nuestros datos de geolocalización ya que se encuentran protegidos por los derechos del secreto de las comunicaciones, intimidad y autodeterminación informativa. Otorgarle esta facultad investigativa exclusivamente a una Unidad Especializada de la Policía, desplazando incluso a la Fiscalía, generará que los medios de prueba obtenidos no puedan ser utilizados en el proceso penal ya que constituyen prueba prohibida. Por otra parte, apostar por relajar las garantías de los ciudadanos en aras de una supuesta eficacia investigativa no hará más que generar impunidad y reforzar aquella inseguridad ciudadana que el Decreto Legislativo pretende combatir. (Elías. R, 2016. p. 8)

Mogrovejo, F. (2019). *El acceso a la Geolocalización por parte de la Policía sin orden Judicial.* Hace referencia a que:

> Los datos que se obtienen a través de la localización y la Geolocalización son parte del paquete de datos de transmisión de información, estos datos están constitucionalmente protegidos, considerados como datos protegidos por el derecho fundamental de la intimidad, así como por el derecho al secreto de las comunicaciones. El Decreto Legislativo N° 1182 no vulnera derechos fundamentales reconocidos por la Constitución Política del Perú, es más presta las garantías necesarias para una investigación adecuada, prevaleciéndose el derecho de defensa del investigado; en

consecuencia, no sería posible indicar que se generar una “prueba prohibida”. (Mogrovejo. F, 2019).

Campos, E. (2019). En su artículo: *Geolocalización del imputado en el Perú, por Edhin Campos Barranzuela.* Hace referencia a que:

> La vigencia del Decreto Legislativo 1322, que tiene la intención de producir un serio descongestionamiento de los establecimientos penitenciarios y, además, constituye un interesante avance en el sistema, que desde luego no se debe abandonar. La geolocalización electrónica, constituye una herramienta poderosa para medir el grado de cumplimiento y readaptabilidad social de los procesados y sentenciados. A decir verdad, la geolocalización de los procesados y sentenciados no es la panacea para prevenir, proteger y resocializarlos, pues pese a tener conocimiento de su ubicación, origen, destino, ruta, hora y fecha de su desplazamiento, nada impide que puedan cometer delitos. (Campos. E, 2019).

Caro, D. (2015). En su artículo: *La Inconstitucionalidad de la Ley de Localización y Geolocalización.* Hace referencia a que:

> El hecho de intervenir comunicaciones para usar datos derivados de estos se encuentra prohibida en el numeral 10 del artículo 2 de la Constitución, que expresamente señala que: *"Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley".* La norma señala que, el acceso a datos de localización y geolocalización sin orden judicial motivada no sólo trae consigo la problemática con respecto al contenido del derecho al secreto de las comunicaciones y la reserva de los documentos privados, sino que también pone de manifiesto cuestiones referidas a la protección de derechos fundamentales tales como la inviolabilidad de la intimidad y la vida privada. La afectación de dichos derechos constitucionales en la obtención de datos de localización y geolocalización sin orden judicial, traerá consigo la imposibilidad de valorar las pruebas obtenidas a partir de dichos datos por considerarse pruebas prohibidas.
>
> De esta forma, quedan en evidencia las ambigüedades, vacíos y contradicciones que trae consigo el Decreto Legislativo N° 1182, cuyo problema central radica en haberse otorgado facultades a la Policía para solicitar la intervención de comunicaciones para la identificación, localización y geolocalización de equipos, sin orden ni control judicial. (Caro. D, 2015)

2.2. Marco Histórico.

En abril 2002: Ley N° 37697. Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos Privados en caso de excepción".

- Otorga al Juez la facultad de conocer y controlar las comunicaciones de las personas investigadas, exclusivamente cuando se trate de los delitos mencionados a continuación: Secuestro, trata de personas, pornografía infantil, robo agravado, extorsión, tráfico ilícito de drogas, tráfico ilícito de migrantes, delitos contra la humanidad, atentados contra la seguridad y traición a la patria, peculado, corrupción de funcionarios, terrorismo, delitos tributarios y aduaneros, lavado de activos y delitos informáticos.

- Otorga al Fiscal de la Nación, Fiscales Penales y Procuradores Públicos la potestad de solicitar al Juez la intervención en los casos antes descritos.

En Julio 2004: Nuevo Código Procesal Penal (NCPP), Artículos 23 y 231: "La intervención de comunicaciones y telecomunicaciones":

- Otorga al Fiscal la potestad de solicitar al Juez la intervención y grabación de comunicaciones cuando sospeche la comisión de un delito cuya pena sea superior a 4 años de prisión y dicha intervención sea absolutamente necesaria para proseguir la investigación. El mandato del juez puede recaer sobre los investigados o personas de su entorno.

- Hace obligatorio para las empresas que ofrecen servicios de telecomunicaciones, facilitar en tiempo real los metadatos de geolocalización de teléfonos móviles y la interceptación y grabación de las comunicaciones ordenadas por mandato judicial de

forma ininterrumpida las 24 horas de los 365 días del año, bajo pena de ser sancionadas.

- Otorga al Fiscal la potestad de conservar las grabaciones hasta que culmine el procesal penal o, al finalizar la investigación si esta no se judicializa, previa autorización del juez.

- Hace obligatorio notificar a él o los investigados sobre todo lo actuado (grabaciones, geolocalización, etc.), solo si el objeto de la investigación lo permite y en tanto esto no ponga en peligro la vida o la integridad corporal de terceros. Para que la intervención se mantenga en secreto será necesario una resolución judicial motivada y con plazo determinado.

En el contexto de aprobación del Decreto Legislativo Nº 1182 promulgado el 27 de julio de 2015, que reguló el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado; las acciones de prevención, investigación y combate de la delincuencia común y el crimen organizado, requerían de un marco regulatorio para fortalecer el ámbito de acción, a través del uso de tecnologías de la información y comunicaciones por parte de la Policía Nacional del Perú para que puedan acceder a los datos telefónicos y de localización y geolocalización ,previa solicitud a los operadores de telefonía autorizados en el país.

El artículo 3 de dicho marco legal, precisa que la unidad de la Policía Nacional del Perú a cargo de la investigación, solicitará a la unidad especializada el acceso inmediato a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar, siempre que concurran los siguientes presupuestos: (a) cuando se trate de flagrante delito, de conformidad con lo dispuesto en el artículo 259 del

Decreto Legislativo Nº 957, Código Procesal Penal, (b) cuando el delito investigado sea sancionado con pena superior a los cuatro años de privación de libertad, (c) el acceso a los datos constituya un medio necesario para la investigación.

El procedimiento para ejecutar las precisiones señaladas, fueron establecidos mediante Resolución Ministerial N° 0631-2015-IN del 16 de octubre del 2015 que aprueba el "Protocolo de Acceso a los Datos de Localización o Geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar" para casos de flagrancia delictiva".

Por su parte el artículo 4 inciso 4.3 del citado decreto legislativo establece el procedimiento para acceder a los datos de la comunicación, obligando a los concesionarios de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, a brindar los datos de localización o geolocalización de manera inmediata las veinticuatro (24) horas del día de los trescientos sesenta y cinco (365) días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento.

La obligatoriedad que establece el: procedimiento mencionado tiene consonancia con las labores que realizan la Fiscalía y el Poder Judicial, quienes convalidan el informe de la policía que sustenta el acceso a los datos de la comunicación. La Fiscalía y la Policía Nacional del Perú están encargadas de investigar y presentar al Juez los hechos que constituyen delito, con base a la información obtenida de los operadores de telecomunicaciones sobre los datos personales solicitados. La información que se solicita siempre es en el marco de una investigación.

Es así que del análisis esgrimido en la exposición de motivos que sustentó la necesidad de contar con un marco legal contenido en el Decreto Legislativo N° 1182, resalta la premisa de: "la preocupación generalizada de los poderes públicos de velar por

la seguridad de los ciudadanos, pues resulta evidente que el crecimiento de las posibilidades de las comunicaciones electrónicas constituyen una herramienta valiosa en la prevención, investigación, detección y enjuiciamiento de delitos, en especial, contra la delincuencia organizada"; no obstante, desde la vigencia del Decreto Legislativo Nº 1182 y el balance de su efectividad refleja algunos vacíos legales que impiden la efectividad y acción rápida de los operadores de justicia que exigen al legislador proponer las mejoras en el ordenamiento jurídico, para la efectiva actuación judicial y operativa de la Policía Nacional.

2.3. Teorías Empleadas.

2.3.1. Tecnologías de Información.

La tecnología como catalizador del cambio: en primer lugar, la aparición de los ordenadores y su incorporación al campo de la Geografía y, en segundo lugar, la aparición de Internet, tanto en el acceso a la información geográfica como en el acceso a herramientas para el tratamiento de esta información. (Ruiz. A, 2010)

El uso de las Tecnologías de la Información y la Comunicación (TICs) y de las Tecnologías de Información Geográfica (TIGs) son dos herramientas básicas para el desarrollo de los territorios hoy en día y una no se entiende sin la otra.

Los datos geográficos pueden incorporarse a estos mapas de muy diversas formas: en diversos formatos como gpx (GPS profesionales), kml/kmz (el formato de Google Earth) o shp (o Shapes, el formato básico de los SIG), a través de servidores web mediante WMS (Web Map Server) o georreferenciando sobre la misma web, mientras que las bases de datos pueden importarse a través del standard csv o xml.

2.3.1.1. Tecnologías de la información y comunicaciones. (TICs)

La expresión TIC, también utilizada como TICs, corresponde a las siglas de Tecnologías de la Información y la Comunicación (en inglés ICT: Information and Communications Technology). Este concepto hace referencia a las teorías, las herramientas y las técnicas utilizadas en el tratamiento y la transmisión de la información: informática, internet y telecomunicaciones.

Existen otros conceptos que hacen referencia a las TIC y que son igualmente aceptados, como NTICS, cuyo significado es Nuevas Tecnologías de la Información y la Comunicación o TI, haciendo referencia a Tecnologías de la Información (del inglés IT: Information Technology). Pero TI nos parece incompleto para referirse a todo el conjunto al que nos referimos, mientras que NTICS no se utiliza con demasiada frecuencia, por lo que lo más habitual es referirse a las TIC o las TICs cuando definimos este concepto.

Las tecnologías de la información y comunicación (TIC) son el resultado de poner en interacción la informática y las telecomunicaciones. Todo, con el fin de mejorar el procesamiento, almacenamiento y transmisión de la información.

Es el conjunto de recursos necesarios para tratar información a través de ordenadores y dispositivos electrónicos, aplicaciones informáticas y redes necesarias para convertirla, almacenarla, administrarla y transmitirla. A nivel de usuario, sea individual o empresa, las TIC forman el conjunto de herramientas tecnológicas que permiten un mejor acceso y clasificación de la información como medio tecnológico para el desarrollo de su actividad.

Las TIC (Tecnologías de la Información y Comunicaciones) son las tecnologías que se necesitan para la gestión y transformación de la información, y muy en

particular el uso de ordenadores y programas que permiten crear, modificar, almacenar, proteger y recuperar esa información. (Daccach, J, 2007)

En este caso, los ordenadores o computadoras son fundamentales para la identificación, selección y registro de la información. De modo particular, subyace un sentido social en el uso de la tecnología, al asociarla a la comunicación, quehacer humano en el cual ineludiblemente se insertan las relaciones sociales.

De esta manera mejorar el nivel de nuestras comunicaciones. Creando nuevas formas de comunicación más rápida y de mayor calidad. Mejoras que reducen costes y tiempo, de aplicación tanto al mundo de los negocios como a la vida misma. Proporcionándonos una mayor comodidad y mejorando nuestra calidad de vida a la vez que se aboga por el medio ambiente. (Bernejo, D, 2021)

2.3.1.1.1. Componentes de las tecnologías de la información y comunicaciones.

Los terminales, las redes y los servicios, por tanto, también pueden ser clasificadas según hagan un uso u otro de estos elementos.

En relación a los dispositivos mucho es lo que se ha avanzado. El ordenador ha evolucionado desde su aparición y sigue haciéndolo a un ritmo vertiginoso. Al igual que los aparatos periféricos que lo complementan, ofreciendo otras posibilidades. (Bernejo, D, 2021)

La tecnología no se ha estancado en los ordenadores. Nos va sorprendiendo introduciendo nuevos tipos de terminales en nuestras vidas o mejorando sus características.

Qué fue de aquel teléfono móvil cuya única función era llamar. Ahora son dispositivos mucho más sofisticados que han revolucionado la comunicación. La vídeo llamada, las aplicaciones de mensajes de texto gratuitas, las redes sociales, etc. son algunos ejemplos. (Bernejo, D, 2021)

En cuanto a las redes que permiten que los dispositivos estén interconectados, la piedra angular sería el internet. Su impacto en la sociedad no se puede explicar en unas líneas, pero es lo que hace girar este mundo. (Bernejo, D, 2021)

Las TICs han hecho un arduo trabajo en el campo de las redes. Mejorando la telefonía fija, la telefonía móvil, el propio internet pasando de la conexión telefónica a la banda ancha, después a la fibra óptica y llevando la conexión a los móviles. Permitiendo así que estemos informados al momento. (Bernejo, D, 2021)

El otro elemento que conforman las tecnologías de la información y la comunicación, son los servicios. Cada vez es más grande el abanico de servicios que se nos ofrece: correo electrónico, búsqueda de información, banca online, comercio electrónico, e-administración, e-gobierno, servicios privados, servicios de ocio, etc.

En España, por ejemplo, existen Entidades Públicas Estatales que se dedican al fomento de las TICs para la realización de trámites administrativos, tanto a nivel privado como público, como pueden ser todas aquellas gestiones que se pueden realizar desde casa con el uso del DNI electrónico. (Bernejo, D, 2021)

2.3.1.1.2. Las TIC desde la perspectiva social.

la introducción de las tecnologías de la información y la comunicación ha traído consigo cambios significativos en la sociedad. La puesta en práctica de las TIC afecta a numerosos ámbitos de la vida humana, en términos teóricos y de gestión cotidiana. (Sánchez, E, 2008)

El uso con sentido apunta a la posibilidad de utilizar efectivamente las TIC, así como saber combinarlas con otras formas de comunicación social. Incluye también la eventualidad de producir contenidos propios, o bien, de acceder a contenidos de otros que resulten útiles. (Sánchez, E, 2008) Es armonizar adecuadamente el recurso Internet con otros, como la radio comunitaria, las reuniones presenciales, los materiales impresos y los videos. Las TIC deben aprovecharse para el desarrollo integral de una comunidad. Una visión integral de desarrollo no implica que se apunte solo hacia el crecimiento económico sino, sobre todo, que impulse el potencial humano en sus diferentes dimensiones para afianzar así la prosperidad económica, pero con equidad, y el fortalecimiento democrático con transparencia y justicia social. (Sánchez, E, 2008)

Es preciso considerar que las TIC no son neutras, positivas o negativas; son simplemente lo que el usuario haga de ellas; no obstante, si quedan oscilando en la nada, pueden favorecer las desigualdades sociales, por lo que es preferible asumirlas con responsabilidad y darles una orientación positiva en beneficio del desarrollo integral de las comunidades. (Sánchez, E, 2008)

Las tecnologías de la información y la comunicación no son suficientes ni imprescindibles para que se dé el desarrollo humano; lo cierto es que,

difícilmente vinieron para no marcharse, por lo que se torna urgente encausarlas para que asuman un papel social al servicio del desarrollo de los pueblos y, ante todo, de los sectores más necesitados. Se entiende que las TIC no siempre son relevantes para transformar la realidad. (Sánchez, E, 2008)

El desafío consiste más bien en discernir cuándo y en qué condiciones pueden aportar al desarrollo. El acceso a las TIC no soluciona con su sola presencia el problema del desarrollo humano, sino que es necesario ir más allá de la conectividad, promoviendo el acceso equitativo, uso y apropiación social de los recursos disponibles. (Sánchez, E, 2008)

Por otro lado, la brecha digital amenaza hoy con incrementar las brechas sociales; esto significa que tenemos que repensar el potencial de las TIC como herramientas que pueden ayudar a construir sociedades más justas, equitativas y democráticas. Hasta aquí tenemos que algunos de los elementos centrales de la visión social de las TIC serían: (Sánchez, E, 2008)

- Ir más allá de la conectividad.
- Propiciar condiciones favorables en el entorno social.
- Minimizar las amenazas y riesgos.
- Potenciar resultados positivos. (Sánchez, E, 2008)

2.3.1.1.3. Amenazas y riesgos en el uso de las TICs.

Ante las posibles consecuencias negativas que el uso de las TIC puede traer para el desarrollo y, frente a estas posibles amenazas y riesgos, diseñar

estrategias que las disminuyan o minimicen. Algunas de estas amenazas o riesgos por considerar son: (Sánchez, E, 2008)

- *Aumento de las desigualdades.* Internet es un medio potencial para aumentar las desigualdades sociales, económicas, culturales y de distinta índole, así como para hacer que las nuevas oportunidades se distribuyan solo entre quienes tienen acceso a ésta. (Sánchez, E, 2008)

- *Homogeneización o imposición.* Contenidos, idioma y cultura, entre otros factores que se privilegian en la Internet, pueden ser negativos al inclinarse, voluntaria o involuntariamente, a uniformar ideas, preferencias y visiones de mundo; descartando o dejando de lado las particularidades de otros pueblos. (Sánchez, E, 2008)

- *Abundancia descontrolada e inmovilización.* Más información no necesariamente equivale a mayor conocimiento. Se corre el riesgo de banalizar o dar una importancia superflua a la información a la que se tiene acceso; al "consumirla" sin analizarla ni reflexionarla. Por otra parte, en lugar de mejorar la vida de la gente, las TIC pueden causar sobrecarga de trabajo, estrés, consumismo y, en general, un lamentable deterioro en la calidad de vida. (Sánchez, E, 2008)

- *Aislamiento y fragmentación.* Las TIC pueden provocar separación y aislamiento. Hay personas y grupos que reducen cada vez más sus intereses y su quehacer cotidiano a pequeños claustros de intercambio cibernético. Solo una ciudadanía informada, organizada y capaz de apropiarse responsable y equitativamente de los recursos de la Internet, puede hacer

frente a las amenazas que implica la introducción de las TIC en la sociedad.

Junto a estos riesgos, es indudable que el uso de las TIC trae o puede traer resultados positivos, como el simplificar y agilizar el acceso a más fuentes de información actualizada; el incremento de formas de intercambio rápidas y a un bajo costo, que permitan la apertura de nuevas ventanas más allá de lo local, el fortalecimiento de una participación consentida e informada, tanto de organizaciones y grupos de la sociedad civil, como de investigadores e investigadoras; quienes rompen así barreras geográficas para ser parte de diálogos, aprendizajes e intercambios, abren la posibilidad de establecer nuevas formas de trabajo colaborativo, redes y alianzas.

Así, las TIC pueden ayudar a personas y organizaciones a fortalecer su imagen y su autoestima; a abrirse espacio y dar a conocer al mundo sus intereses y prioridades. En el campo de la educación, las TIC tienen la posibilidad de aportar a la formación; pueden incentivar a muchas personas para que regresen a estudiar y para que mejoren la lectura y la escritura, entre otras alternativas.

En términos generales, las TIC pueden devenir en un apoyo para que muchos se sientan parte activa y capaz de una sociedad que sistemáticamente les ha excluido y explotado, es el caso, por ejemplo, de los pueblos indígenas. (Sánchez, E, 2008)

2.3.1.1.4. Aportaciones de las TICs a las empresas.

- *A nivel de información:* Reduce costes y mejora el uso y la transmisión de la misma.

- *Nivel de estructura de empresa:* Mejora la comunicación y relaciones personales de los trabajadores.

- A nivel comercial: Extensión del mercado (comercio electrónico), disminución de costes logísticos, facilita el feedback con los clientes y mejora la imagen de marca. Las tecnologías de la información y la comunicación son una herramienta que sirve para hacer más fácil y cómoda nuestra vida, tanto a nivel personal como profesional y, además, le da un poco de aliento a nuestro planeta. Por tanto, por qué no dar luz verde a estos avances. (Bernejo, D, 2021)

2.3.1.2. Tecnología de la información geográfica. (TIGs)

Las Tecnologías de la Información Geográfica (TIG), concretamente los Sistemas de Información Geográfica, la Teledetección, la Cartografía digital, los GPS o la Fotogrametría constituyen una nueva ciencia en creciente expansión, debido a su variabilidad en su aplicación con ámbitos tan distintos como el medio ambiente y los recursos naturales, la demografía, la gestión de servicios públicos, el urbanismo, la ordenación del territorio, la planificación del transporte, el geomarketing, etc.

Las Tecnologías de la Información Geográfica (TIG) nos permiten asociar a la representación gráfica de cualquier lugar del planeta todos aquellos datos que consideremos interesantes, de forma que podamos analizar diferentes parámetros o

estudiar distintos aspectos sobre los objetos, fenómenos o acontecimientos que tienen lugar en cualquier territorio, así como las relaciones entre ellos. Las ventajas que esto supone para conseguir un conocimiento más preciso y para aumentar la eficacia en la gestión de una región, de sus recursos y de las actividades que en ella se pueden desarrollar, hacen de las TIG un instrumento imprescindible en prácticamente cualquier ámbito de trabajo, y por supuesto en la cooperación al desarrollo.

En los últimos años, todas las tecnologías asociadas a la información geográfica han tenido una gran evolución, principalmente, gracias al desarrollo de Internet. El uso social de la Red se ha traducido en nuevas iniciativas y proyectos que tienen como fundamento principal poder compartir recursos: los servidores de mapas, las bases de datos distribuidas, y todo un conjunto de tecnologías que permiten la interoperabilidad entre sistemas.

Estos avances van llegando poco a poco a las ONGD, sin embargo, el nivel de formación y de utilización en general, dista mucho de las capacidades que ofrecen estas tecnologías en los proyectos de cooperación al desarrollo. En el presente Cuaderno, expertos y usuarios de las TIG comparten conocimientos y experiencias prácticas que nos pueden ayudar a potenciar estas herramientas en los proyectos que elaboremos desde nuestras organizaciones. (Puig, C y Valera A, 2008)

2.3.1.2.1. Técnicas utilizadas en los sistemas de información geográfica.

2.3.1.2.1.1. La creación de datos.

Las modernas tecnologías SIG trabajan con información digital, para la cual existen varios métodos utilizados en la creación de datos digitales. El

método más utilizado es la digitalización, donde a partir de un mapa impreso o con información tomada en campo se transfiere a un medio digital por el empleo de un programa de Diseño Asistido por Ordenador (DAO o CAD) con capacidades de georreferenciación.

Dada la amplia disponibilidad de imágenes orto-rectificadas (tanto de satélite y como aéreas), la digitalización por esta vía se está convirtiendo en la principal fuente de extracción de datos geográficos.

Esta forma de digitalización implica la búsqueda de datos geográficos directamente en las imágenes aéreas en lugar del método tradicional de la localización de formas geográficas sobre un tablero de digitalización. (Wikipedia, s.f.)

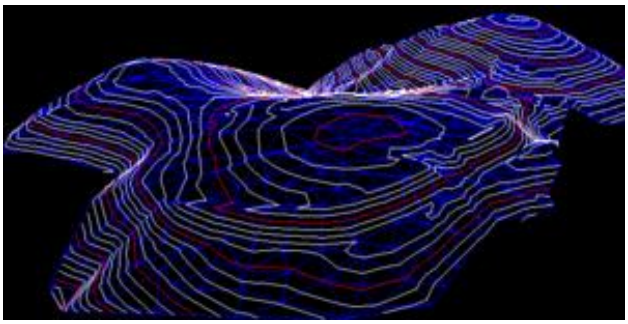
2.3.1.2.1.2. La representación de los datos.

Los datos SIG representan los objetos del mundo real (carreteras, el uso del suelo, altitudes). Los objetos del mundo real se pueden dividir en dos abstracciones: objetos discretos (una casa) y continuos (cantidad de lluvia caída, una elevación). Existen dos formas de almacenar los datos en un SIG: raster y vectorial. (Wikipedia, s.f.)

- *Raster.* Un tipo de datos raster es, en esencia, cualquier tipo de imagen digital representada en mallas. El modelo de SIG raster o de retícula se centra en las propiedades del espacio más que en la precisión de la localización. Divide el espacio en celdas regulares donde cada una de ellas representa un único valor. Se trata de un modelo de datos muy adecuado para la representación de variables continuas en el espacio.

- *Vectorial.* En un SIG, las características geográficas se expresan con frecuencia como vectores, manteniendo las características geométricas de las figuras. En los datos vectoriales, el interés de las representaciones se centra en la precisión de la localización de los elementos geográficos sobre el espacio y donde los fenómenos a representar son discretos, es decir, de límites definidos. Cada una de estas geometrías está vinculada a una fila en una base de datos que describe sus atributos. (Wikipedia, s.f.)

Figura: N° 1. Representación vectorial



Fuente: Sistema de información geográfica (Wikipedia, s.f.)

Por ejemplo, una base de datos que describe los lagos puede contener datos sobre la batimetría de estos, la calidad del agua o el nivel de contaminación. Esta información puede ser utilizada para crear un mapa que describa un atributo particular contenido en la base de datos. Los lagos pueden tener un rango de colores en función del nivel de contaminación. Además, las diferentes geometrías de los elementos también pueden ser comparadas. Así, por ejemplo, el SIG puede ser usado para identificar aquellos pozos (geometría de puntos) que están en torno a 2 kilómetros de un lago (geometría de polígonos) y que tienen un alto nivel de contaminación. (Wikipedia, s.f.)

2.3.1.2.1.3. Captura de dados.

La captura de datos, y la introducción de información en el sistema consume la mayor parte del tiempo de los profesionales de los SIG. Hay una amplia variedad de métodos utilizados para introducir datos en un SIG almacenados en un formato digital. (Wikipedia, s.f.)

Los datos impresos en papel o mapas en película PET pueden ser digitalizados o escaneados para producir datos digitales.

Con la digitalización de cartografía en soporte analógico se producen datos vectoriales a través de trazos de puntos, líneas, y límites de polígonos. Este trabajo puede ser desarrollado por una persona de forma manual o a través de programas de vectorización que automatizan la labor sobre un mapa escaneado.

No obstante, en este último caso siempre será necesario su revisión y edición manual, dependiendo del nivel de calidad que se desea obtener. (Wikipedia, s.f.)

Los datos obtenidos de mediciones topográficas pueden ser introducidos directamente en un SIG a través de instrumentos de captura de datos digitales mediante una técnica llamada geometría analítica.

Además, las coordenadas de posición tomadas a través un Sistema de Posicionamiento Global (GPS) también pueden ser introducidas directamente en un SIG. (Wikipedia, s.f.)

2.3.1.2.1.4. Análisis espacial mediante SIG.

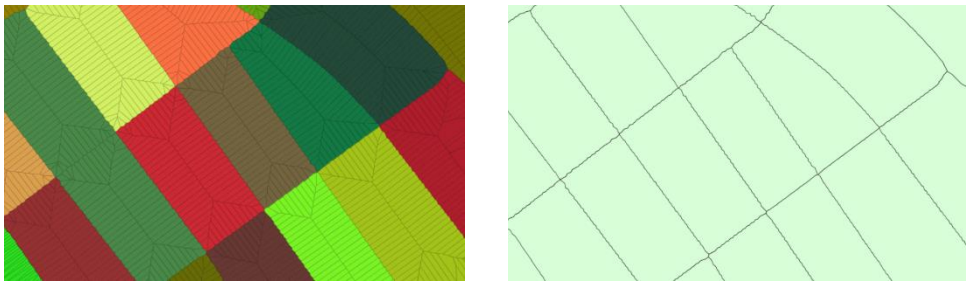
Dada la amplia gama de técnicas de análisis espacial que se han desarrollado durante el último medio siglo, cualquier resumen o revisión sólo puede cubrir el tema a una profundidad limitada.

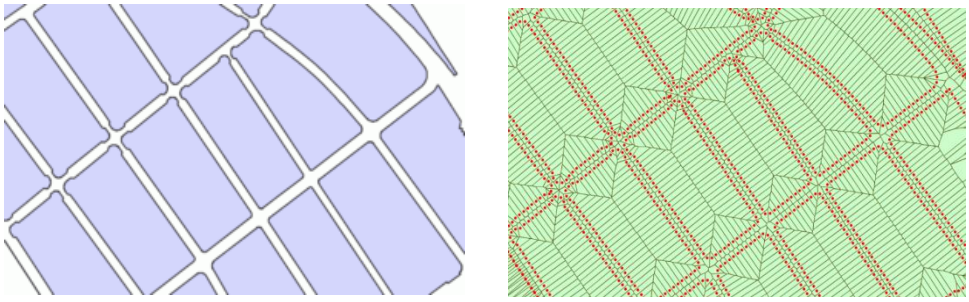
Este es un campo que cambia rápidamente y los paquetes de software SIG incluyen cada vez más herramientas de análisis, ya sea en las versiones estándar o como extensiones opcionales de este.

En muchos casos tales herramientas son proporcionadas por los proveedores del software original, mientras que en otros casos las implementaciones de estas nuevas funcionalidades se han desarrollado y son proporcionados por terceros.

Además, muchos productos ofrecen kits de desarrollo de software (SDK), lenguajes de scripting, etc. para el desarrollo de herramientas propias de análisis u otras funciones. (Wikipedia, s.f.)

Figura N° Proceso llevado a cabo en un SIG. (Sistema de Información Geográfica)





Fuente: Sistema de información geográfica. (Wikipedia, s.f.)

2.3.1.2.1.5. Geocodificación.

Geocodificación es el proceso de asignar coordenadas geográficas (latitud-longitud) a puntos del mapa (direcciones, puntos de interés, etc.). Uno de los usos más comunes es la georreferenciación de direcciones postales. Para ello se requiere una cartografía base sobre la que referenciar los códigos geográficos. Esta capa base puede ser, por ejemplo, un tramero de ejes de calles con nombres de calles y números de policía. Las direcciones concretas que se desean georreferenciar en el mapa, que suelen proceder de tablas tabuladas, se posicionan mediante interpolación o estimación. El SIG a continuación localiza en la capa de ejes de calles el punto en el lugar más aproximado a la realidad según los algoritmos de geocodificación que utiliza.

La geocodificación puede realizarse también con datos reales más precisos (por ejemplo, cartografía catastral). En este caso el resultado de la codificación geográfica se ajustará en mayor medida a la realizada, prevaleciendo sobre el método de interpolación.

En el caso de la geocodificación inversa el proceso sería al revés. Se asignaría una dirección de calle estimada con su número de portal a unas coordenadas x, y determinadas.

Por ejemplo, un usuario podría hacer clic sobre una capa que representa los ejes de vía de una ciudad y obtendría la información sobre la dirección postal con el número de policía de un edificio.

Este número de portal es calculado de forma estimada por el SIG mediante interpolación a partir de unos números ya presupuestos. Si el usuario hace clic en el punto medio de un segmento que comienza en el portal 1 y termina con el 100, el valor devuelto para el lugar seleccionado será próximo al 50. Hay que tener en cuenta que la geocodificación inversa no devuelve las direcciones reales, sino sólo estimaciones de lo que debería existir basándose en datos ya conocidos. (Wikipedia, s.f.)

2.3.2. Geolocalización.

2.3.2.1. Definición.

La geolocalización es una herramienta utilizada por los geógrafos para situar a las personas u objetos en el espacio mediante sus coordenadas y que ha cobrado una nueva dimensión a partir de la aparición de Internet y de los dispositivos móviles. (Beltrán, G, 2015)

Existe una confusión entre términos muy semejantes pero que son distintos: geolocalización es un término que se ha puesto de moda en Internet, utilizado muchas veces de forma similar a geoposicionamiento y georreferenciación; GPS como acrónimo de Global Positioning System (Sistema de Posicionamiento

Global) y localización como un aspecto más genérico.

GPS: Sistema que permite conocer la posición de un objeto móvil gracias a la recepción de señales emitidas por una red de satélite. Es un sistema global de navegación por satélite. Permite determinar la posición de un objeto o persona, en todo el mundo variando tan solo por metros. En la actualidad su operación lo maneja el Gobierno de Estados Unidos, bajo el control de Departamento de Defensa. (Badillo, J. Domingo, P. & Gonzales, I, 2018)

GSM. Sistema Global para las comunicaciones Móviles. (Global System, for Mobile Communications), se basa en la utilización de redes telefónicas en general. Se maneja por medio de las antenas de telecomunicaciones, las cuales sirven para que los teléfonos tengan cobertura.

La geolocalización es un concepto que hace referencia a la situación que ocupa un objeto en el espacio y que se mide en coordenadas de latitud (x), longitud (y) y altura (z). Por tanto, se utiliza el neologismo geolocalización como expresión popular más difundida de la localización de personas, objetos o cosas mediante el uso de un sistema GPS o similar.

2.3.2.2. Ventajas.

La geolocalización ayuda a identificar la ubicación geográfica real de los objetos, como dispositivos móviles o cualquier terminal conectada a Internet. El término "geolocalización" se refiere tanto al proceso de localización geográfica de los objetos como a la ubicación geográfica real identificada.

La geolocalización es una tecnología que ofrece información en un doble sentido, nosotros como usuarios nos beneficiamos de la información que nos

facilita. Muchas tareas sin esta tecnología serían más complicadas de realizar como obtener la ruta más corta a nuestro destino, o directamente imposibles como conocer el punto exacto dónde está el último paquete que hemos comprado por Internet.

Pero este flujo de información también viaja en sentido contrario, nosotros facilitamos información de manera constante sobre nuestra ubicación. Cuando publicamos en redes sociales utilizando la funcionalidad de geoposicionamiento o cuando damos permisos a una app de nuestro smartphone para acceder a nuestra ubicación estamos facilitando información personal sobre nuestros hábitos diarios relativos a rutas, lugares que visitamos o similar.

Esta información generalmente es beneficiosa para ambos ya que nosotros obtenemos herramientas con las que interactuar optimizando muchas tareas y las organizaciones y desarrolladores de apps obtienen valiosa información con la que mejorar la experiencia del usuario. Algunas aplicaciones de esta tecnología son:

- Obtener resultados de una búsqueda basados en la ubicación.
- Publicidad personalizada en función de tu ubicación.
- Pedir ayuda en caso de emergencia.
- Dar a conocer en redes sociales la ubicación de una foto o un video.
- Analizar el comportamiento de los usuarios para mejorar la “experiencia de uso”.
- Realizar estudios con los que mejorar una tecnología existente o crear una nueva; etc.

2.3.2.3. Riesgos.

Los usos descritos anteriormente y otros muchos que no hemos indicado relativos a la geolocalización, también pueden tener consecuencias negativas. Cualquier información de carácter personal puede comprometer nuestra privacidad y los datos de geolocalización son de este tipo.

La geolocalización y las aplicaciones de mapas son usados más comúnmente de los que pensamos para realizar acciones delictivas. Los delincuentes utilizan estas herramientas para encontrar objetivos potenciales basándose por ejemplo en las publicaciones que hacemos en redes sociales o la información facilitada por mapas virtuales como Google Maps.

2.3.2.4. Geolocalización sin control.

El método para exigir el levantamiento del secreto de las telecomunicaciones con el objetivo de búsqueda criminal se encontraba sujeto al consentimiento de un juez que catalogaba a la legitimidad de la medida y especificaba cabalmente el periodo y los efectos de la misma. De esta manera, podía decirse que la afectación de la privacidad estaba demostrada por fuertes signos de que el intervenido había cometido un delito establecido por un tercero imparcial. (Neciosup. S, 2017)

Bajo la excusa; sin embargo, de que este procedimiento de control judicial registraba mucho tiempo y hacía incapaz la labor policial, el dl 1182 establece que dicho control sea posterior. Es decir, siempre que se realicen tres supuestos:

- Cuando exista flagrancia,
- Se investigue un delito sancionado con más de 4 años de prisión.

- El acceso a los datos de geolocalización sea severamente fundamental. (Neciosup. S, 2017)

Mientras tanto, la policía podrá “saltarse” el control y tendrá hasta 72 horas antes de que un juez se percate de los hechos tomados y las declare válidas o no. En la práctica, esto significa que la afectación de la privacidad ya no es elegible, sino que es total. El estado tiene que defendernos y a cambio anuncia aceptemos saber por dónde estamos en cualquier instante. (Neciosup. S, 2017)

Estas conjeturas, que podrían sonar hasta cierto punto válido, carecen de diferentes problemas. Quizás el más evidente es que ni el texto de la ley ni la exposición de motivos muestran una sola cifra que nos manifieste cuántos delitos dejarían de perpetrarse o con qué regularidad la policía pide esta noticia para solucionar sus casos. (Neciosup. S, 2017)

2.3.2.5. Decreto Legislativo N° 1182 Ley Stalker.

El 27 de julio de 2015 se publicó el Decreto Legislativo 1182, que regula el acceso y posterior uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de telefonía móvil y dispositivos electrónicos afines, en la lucha contra la delincuencia y el crimen organizado. Además, entre otros ajustes legislativos, crea un mandato de retención y conservación de datos derivados de las telecomunicaciones por un plazo de hasta treinta y seis (36) meses.

Permite que los policías sepan dónde estás sin pedirle permiso a nadie, sin ninguna orden judicial. Sí, tal y como suena, bajo la excusa de que “el Poder Judicial la hace muy larga”. (Caballero. V, 2015)

“El Decreto Legislativo N° 1182, busca regular el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación en la lucha contra la delincuencia y el crimen organizado. Aunque introduce también otras modificaciones al Código Penal, la parte más problemática es la de sus nueve artículos principales en la que crea dos nuevos mecanismos de acceso a la información privada de los ciudadanos”. (Caballero. V, 2015)

El Decreto Legislativo crea un mecanismo mediante el cual la Policía puede enviar un pedido a cualquier empresa operadora para acceder a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos. Estos datos son enviados permanentemente por todos los teléfonos móviles conectados a una red de comunicaciones, incluso los que no son smartphones, y constituyen un registro exacto de la circulación de cualquier usuario de estos aparatos. (Caballero. V, 2015)

En una de sus tantas disposiciones complementarias, la Ley Stalker realiza el mayor cambio en cuanto a la protección de la privacidad de la historia: toda nuestra información será almacenada por tres años. “Una norma expresa que obliga a todas las empresas concesionarias de servicios públicos a almacenar por tres años toda la información de los datos derivados de las telecomunicaciones para que pueda ser consultada por la Policía.

Esto significa que toda la información sobre los detalles de con quién nos comunicamos, por cuánto tiempo, y desde dónde, entre otros, correspondientes a los últimos tres años serán almacenados por las empresas de telecomunicaciones”.

Gráfico N° 1. La Geolocalización

Fuente: (Caballero. V, 2015)

Para acceder a esta información mucho más detallada, el decreto establece que sí es necesario una autorización por parte del Poder Judicial.

Sin embargo, esto no es suficiente, ya que el simple acto de almacenar tanto tiempo este tipo de información viola la privacidad de los ciudadanos.

Incluso hay todo un principio internacional sobre la aplicación de los derechos Humanos a la vigilancia de las comunicaciones. (Caballero. V, 2015)

2.3.2.5.1. Requisitos para que la Policía conozca los datos personales.

Para que la policía sepa tu ubicación satelital, se necesita el cumplimiento de tres requisitos.

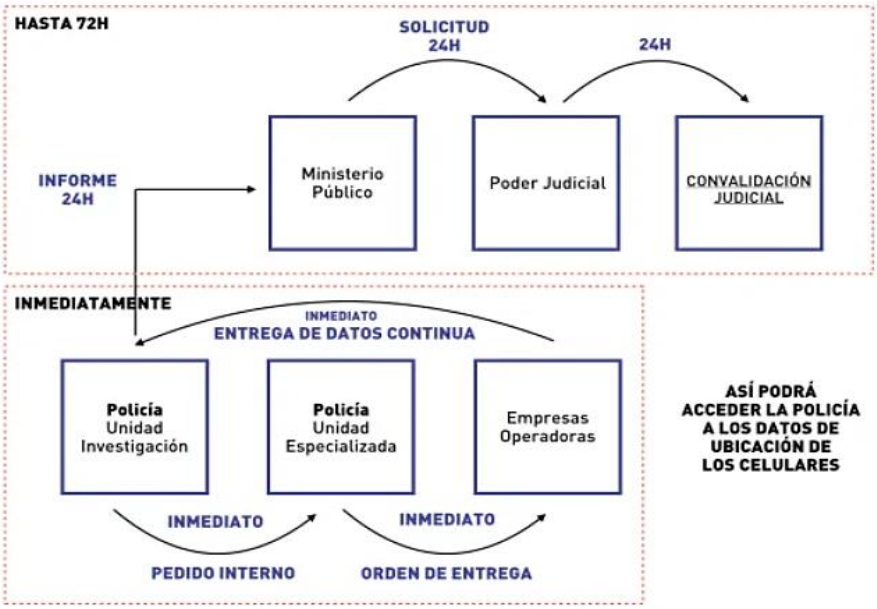
- *Se trata de un delito flagrante.*
- *El delito investigado será sancionado con una pena igual o mayor a los cuatro años de cárcel.*

- *El acceso a esta información sea un medio fundamentalmente necesario para la investigación.*

Pero aquí es donde comienza lo realmente preocupante, el cumplimiento de estos requisitos sólo será revisado cuando la policía ya haya accedido a la información.

Luego, la PNP tendrá 24 horas para enviar al Fiscal un informe que sustente el requerimiento y el Fiscal tendrá otras 24 horas para solicitarle al juez la "convalidación de la medida" y el juez tendrá otras 24 horas para pronunciarse sobre la legalidad del pedido y establecer un periodo durante el cual estará vigente. (Caballero. V, 2015)

Gráfico N° 2 Procedimiento.



Fuente: (Caballero. V, 2015)

La policía pedirá el acceso a tu ubicación y tu identidad y luego tendrá que explicar por qué la pidió. Pasarán 72 horas hasta que un juez decida si era necesario pedir información y verifique si todos los requisitos han sido respetados.

Haya sido necesario o no, igual el policía ya sabrá que tú eres el dueño de la línea y dónde estuviste. (Caballero. V, 2015)

Bajo el esquema anteriormente vigente, si la Policía quería necesitaba acceder a la geolocalización de cualquier línea telefónica era necesario que sea un Fiscal quien se lo solicite a un Juez.

Resultaba responsabilidad del Fiscal convencer al Juez de que existían indicios suficientes como para amparar esta solicitud y era el magistrado quien establecía la forma, oportunidad, periodo y garantías aplicables a la intervención. (Caballero. V, 2015)

Gráfico N° 2. Consecuencias que acarrea la norma.

Fuente: (Hiperderecho, 2015).

Se implementan con el fin de obtener información en tiempo real que facilite principalmente la investigación de los delitos, pero también se pueden emplear para la ubicación de personas desaparecidas, el seguimiento de actividades posiblemente delictivas, la represión de activistas y líderes de movimientos sociales, entre otros.

El Decreto Legislativo afecta derechos fundamentales El artículo 6 del Decreto Legislativo precisa que se "***excluyen expresamente cualquier tipo de intervención de las telecomunicaciones, las que se rigen por los procedimientos correspondientes."*** Es decir, el Ejecutivo trata de evitar cuestionamientos relacionados a la restricción de derechos fundamentales en la búsqueda y obtención de medios de pruebas. Sin embargo, se considera que sí se afectan tanto el derecho al secreto de las comunicaciones (artículo 2.10 Const.), a la intimidad (artículo 2.7 Const.) como a la autodeterminación informativa (artículo 2.6 Const.). (Elías. R, 2016. p. 8)

Pese a que esto, sí es necesario advertir que el Estado, al ordenar que se efectúe una audiencia de convalidación de la facultad policial, reconoce que se están afectando derechos fundamentales pues, de lo contrario, esta diligencia sería innecesaria.

No se debe olvidar que con las nuevas tecnologías lo que se transmite no sólo es el contenido (mensaje) sino también información relacionada al emisor, sea de manera consciente o inconsciente. Así, al inicio, cada llamada o mensaje que enviamos a través de las redes móviles o las nuevas tecnologías está compuesta por datos de información de la transmisión y de contenido. Si se justifica realizar un trato diferenciado entre ambas pues la exigencia será mucho mayor en el caso de una intervención telefónica y menor cuando se requiera la ubicación del dispositivo. Esto no justifica excluir de su protección a una de ellas.

Al tratar de demostrar que es imposible jurídicamente que se encuentre ante supuestos de flagrancia que habiliten la geolocalización del presunto agente, ya que dicha figura requiere dos elementos***: inmediatez temporal e inmediatez personal. Este último no se encuentra presente en los delitos cometidos a través de dispositivos***

móviles o similares. Prescindir de la inmediatez personal ampliaría peligrosamente la figura de flagrancia delictiva. (Elías. R, 2016. p. 8)

Por otro lado, ***el Decreto Legislativo no restringe la geolocalización a casos de extorsión, trata de personas u otros delitos muy graves*** como fue planteada inicialmente, sino virtualmente a todo tipo de delitos previstos en el Código Penal. Además, ***el Decreto Legislativo exige que sea el Policía y no el Fiscal quien evalúe la necesidad, sub-principio que integra el principio de proporcionalidad, de restringir un derecho fundamental; es decir, propicia la confusión jurídica de roles.*** (Elías. R, 2016. p. 8)

En primer lugar, la única posibilidad de aplicar el Decreto Legislativo es eliminando (peligrosamente) la inmediatez personal como requisito de la flagrancia delictiva. En efecto, respecto al primer requisito, el Tribunal Constitucional ha establecido que de manera copulativa y no disyuntiva debe de reunirse criterios de inmediatez temporal y personal para su aplicación.

De esta forma, el Supremo Intérprete en los pronunciamientos más recientes ha establecido: 26 (…) que la flagrancia en la comisión de un delito presenta la concurrencia de dos requisitos insustituibles: ***a) la inmediatez temporal, es decir, que el delito se esté cometiendo o que se haya cometido antes; y b) la inmediatez personal,*** es decir, que el presunto delincuente se encuentre en el lugar de los hechos en el momento de la comisión del delito y esté relacionado con el objeto o los instrumentos del delito, ofreciendo una prueba evidente de su participación en el hecho delictivo.”

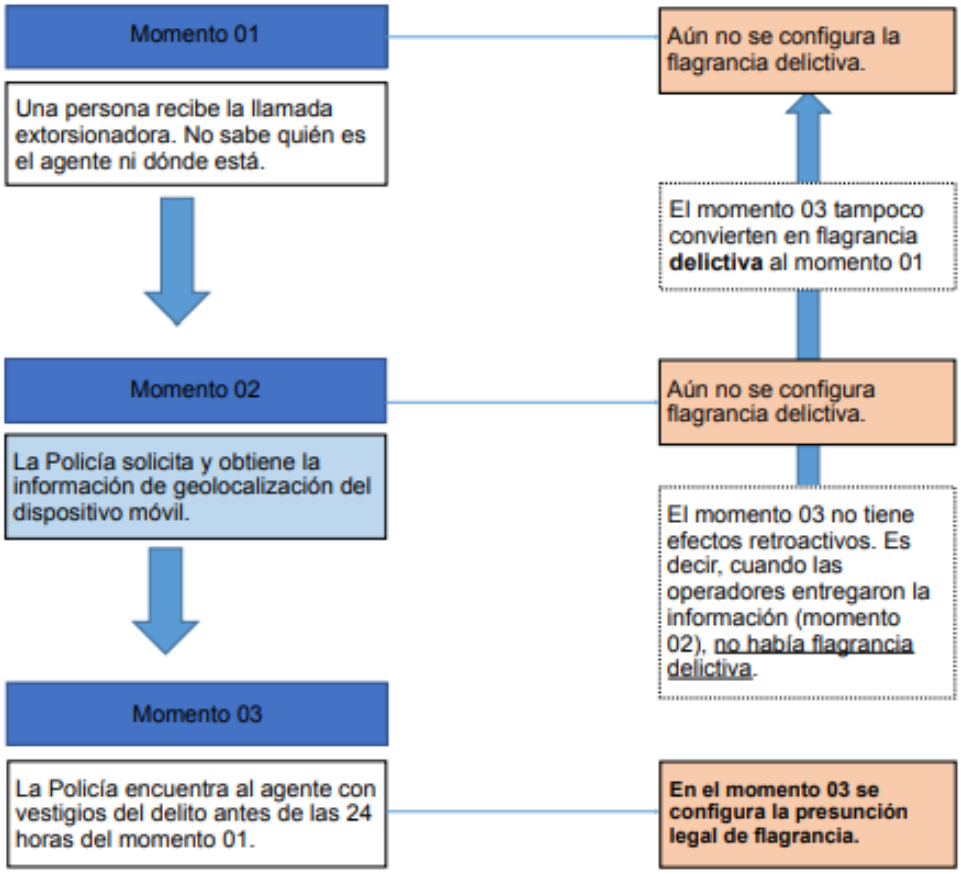
Al analizar los cuatro supuestos de flagrancia previstos en el artículo 259 del Código Procesal Penal caemos en cuenta que estos no cobijan aquellos casos para los que el Decreto Legislativo fue promulgado.

Ejemplo: acabamos de recibir una llamada exigiéndonos un monto de dinero para que nuestro negocio no sea incendiado. La pregunta es: ¿en cuál de los cuatro supuestos de flagrancia nos encontramos: ¿flagrancia clásica, cuasifagrancia, flagrancia por indicios o presunción de flagrancia?

- No nos encontramos frente a la flagrancia clásica o flagrancia propiamente dicha pues el agente no ha sido descubierto mientras está realizando el hecho punible. Es más, no sabemos quién es este mientras se lleva a cabo la llamada.
- El agente tampoco ha sido descubierto después de la realización del hecho punible. Nuevamente, lo que el binomio Policía / Fiscalía deben hacer es identificar al responsable del delito pero la mera recepción de la llamada –o mensaje de texto, WhatsApp, etc.– no posibilita en sí su descubrimiento. Este es un círculo vicioso pues para emplear la geolocalización del dispositivo necesitaríamos haber localizado previamente al agente pues, de lo contrato, el agente no habría sido descubierto y, por lo tanto, no nos encontraríamos en un supuesto de flagrancia.
- Ni el agraviado ni otra persona y mucho menos un dispositivo audiovisual ha identificado al agente durante o inmediatamente después de la comisión del hecho delictivo. En consecuencia, no nos encontramos ante este supuesto de flagrancia por indicios.
- Finalmente, la presunción legal de flagrancia tampoco se da ya que el agente no ha sido encontrado con vestigios de la comisión del delito. ***Este supuesto se***

aplica cuando el agente ya fue identificado y ubicado por la Policía y, por tanto, puede ser detenido. En el caso de la geolocalización, no podemos decir que se encontró al agente, sino que podría ser encontrado si se accede a la ubicación del dispositivo y eso no es flagrancia.

Para demostrar que recién estaremos en flagrancia si se encuentra al agente con vestigios del delito. Esto significa que cuando la Policía solicita la geolocalización aún no se encuentra en flagrancia ya que la figura procesal no puede legitimar acciones anteriores a su configuración.



Fuente: (Elías. R, 2016. p. 8)

La geolocalización sí permitiría encontrar al agente, incluso, dentro de las 24 horas de su comisión, pero no por encontrarse en un supuesto de flagrancia sino ante la

comisión de un delito que merece ser investigado a través de búsqueda de pruebas con restricción de derechos, lo cual requiere autorización judicial previa.

Considerar que nos encontramos ***ante un delito flagrante sería restringir esta categoría procesal a la inmediatez temporal y prescindir de la inmediatez personal.*** Ello, sin duda, sería relajar las garantías procesales de todo ciudadano. ***Si se quiere invocar casuística, debemos tener presente que, de acuerdo a lo reportado por la Policía Nacional, el primer caso de empleo de geolocalización ante un (imposible) flagrante delito se trató de un "auto secuestro." El secuestro era una farsa. En consecuencia, tanto la Policía que solicitó y accedió como la operadora que brindó información, lesionaron derechos fundamentales de un ciudadano.*** (Elías. R, 2016. p. 8)

En segundo lugar, el Ejecutivo planteó la facultad legislativa como una propuesta excepcional para combatir casos de sicariato, extorsión, tráfico ilícito de drogas e insumos químicos, usurpación, tráfico de terrenos y tala ilegal de madera, pero la redacción del Decreto Legislativo permite solicitar la geolocalización, sin autorización judicial, de prácticamente cualquier delito previsto en el Código Penal. Si concordamos el artículo 6.2 con el artículo 1 del Decreto Legislativo tenemos que esta norma se aplica tanto a la delincuencia común como al crimen organizado; es decir, a todo el catálogo de delitos del Código Penal.

En vez de seleccionar un grupo específico de delitos en los que se podría aplicar la geolocalización, como el en caso de la interferencia de las comunicaciones, el Ejecutivo aprobó que sea aplicable a todos los ilícitos sancionados con pena superior a cuatro años de privación de libertad.

De este modo, los delitos que posibilitan la geolocalización sin autorización judicial no se reducen a aquellos catalogados como graves pues esta herramienta también podría emplearse ante casos de estafa, corrupción de funcionarios, fraude informático, fraude en la administración de personas jurídicas, ultraje a los símbolos patrios, y un largo etcétera.

Como puede apreciarse, al no existir una clara restricción, posibilita la ubicación en tiempo real de cualquier ciudadano que cuente con un dispositivo electrónico y que haya sido denunciado ante la Policía.

En tercer lugar, la norma exige que el acceso a los datos constituya un medio necesario para la investigación. Este extremo está relacionado con el sub-principio de necesidad que forma parte del principio constitucional de proporcionalidad, exigido cuando se deben adoptar acciones que restringen derechos fundamentales.

Siendo esto así, nos debemos preguntar: ¿a quién le corresponde realizar el análisis jurídico constitucional para la restricción de derechos en la búsqueda de pruebas? ¿A la Policía o a la Fiscalía?

Es la Constitución la que posibilita excepcionalmente que la Policía pueda realizar este tipo de actos, pero únicamente en dos casos concretos: detención (artículo 2.24.f Const.) y allanamiento (artículo 2.9 Const.). De esta manera, para la afectación al secreto de las comunicaciones, se requiere autorización judicial previa.

El Decreto Legislativo no puede legitimar una restricción constitucional tan grave.

a) El Procedimiento inconstitucional que merma la función del fiscal en el conocimiento e investigación del delito.

Los artículos 4 y 5 del Decreto Legislativo regulan el procedimiento policial para acceder a la ubicación de los dispositivos electrónicos y el pedido de convalidación judicial. Los pasos que sigue este procedimiento especial y demostraremos que existen vicios: el sacrificio de garantías en aras de una supuesta eficacia investigativa.

i. ***La unidad a cargo de la investigación policial***, una vez verificados los supuestos del artículo***, pone en conocimiento del Ministerio Público el hecho y formula el requerimiento a la unidad especializada de la Policía Nacional del Perú para efectos de la localización o geolocalización*** (artículo 4.1). *La norma condiciona la puesta en conocimiento de los hechos denunciados a una previa verificación a cargo de la Policía de los supuestos, que, impide tratar los delitos cometidos a través de dispositivos móviles bajo la figura de flagrancia delictiva. Dicho de otro modo, la redacción es tendenciosa pues,* ***de acuerdo al artículo 331.1 del Código Procesal Penal, la Policía debe de comunicar inmediatamente la denuncia formulada por un ciudadano ante su dependencia y no condicionarlo a la verificación previa de los referidos supuestos.*** (Elías. R, 2016)

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

(artículo 4.2). Los argumentos por los que la Policía no tiene la facultad constitucional de solicitar datos de localización o geolocalización a las empresas de comunicación al encontrarse protegidas por el derecho fundamental del secreto de las comunicaciones. ***No se ha tenido acceso al protocolo que regula el procedimiento que estamos analizando; sin embargo, la Policía ya hace uso de esta facultad***. Se espera que todo el circuito de comunicación ***-desde el registro de la denuncia, la comunicación al Ministerio Público, así como a la Unidad Especializada, la verificación del responsable hasta los correos electrónicos de solicitud y de respuesta de las operadoras- se encuentre anexo a la carpeta fiscal*** pues, de lo contrario, se estaría restringiendo el derecho a la defensa ya que no tendría la posibilidad de verificar cómo se desarrolló el procedimiento. (Elías. R, 2016)

iii. Los concesionarios o servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, están obligados a brindar los datos de localización o geolocalización de manera inmediata, las veinticuatro (24) horas del día de los trescientos sesenta y cinco (365) días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento (artículo 4.3). Sé que el término "inmediato" aumenta los riesgos al condicionar la aplicación de esta facultad excepcional a casos de flagrancia.

Ejemplo.: El 1 de enero de 2016 a las 00:00 recibimos una llamada extorsionadora. Acudimos a la Policía a las 18:00, mientras se realizan las comunicaciones respectivas pasan algunas horas y la Unidad Especializada remite la comunicación a la operadora a las 23:00 y esta responde a las

01:00. A quienes aún consideren que sólo se requiere inmediatez temporal y no personal para la configuración de la flagrancia, la pregunta es ¿qué harían con la información recibida pues aun cuando encontrasen al agente? Al haber pasado más de 24 horas, este no podrías detenido. Es más, habrían recibido la información cuando la flagrancia (que se considera no se configura) ya habría cesado. (Elías. R, 2016)

iv. La unidad a cargo de la investigación policial realiza las diligencias pertinentes en consideración de la información obtenida y a otras técnicas de investigación, sin perjuicio de lo establecido en el artículo 5 (artículo 4.4). ***Que la Policía realice actos de investigación no genera problema alguno, pues forman parte de sus funciones conforme se encuentra previsto en el artículo 67 del Código Procesal Penal.***, salvo detención policial o allanamiento en flagrancia, no está facultada constitucionalmente a restringir nuestro derecho al secreto de las comunicaciones. (Elías. R, 2016)

v. La unidad policial a cargo de la investigación policial, dentro de las 24 horas de comunicado el hecho al Fiscal correspondiente, le remitirá un informe que sustente el requerimiento para su convalidación judicial (artículo 5.1***). El Fiscal dentro de las veinticuatro (24) horas de recibido el informe, solicita al Juez la convalidación de la medida (artículo 5.2). La redacción es inadecuada y sugiere que en todos los casos el Fiscal solicitará la convalidación judicial. Nuevamente, el titular de la acción penal es el Fiscal y, de acuerdo al artículo 60.2 del Código Procesal Penal: "El Fiscal conduce desde su inicio la investigación del delito. Con tal propósito la Policía Nacional está obligada a cumplir los mandatos del Ministerio***

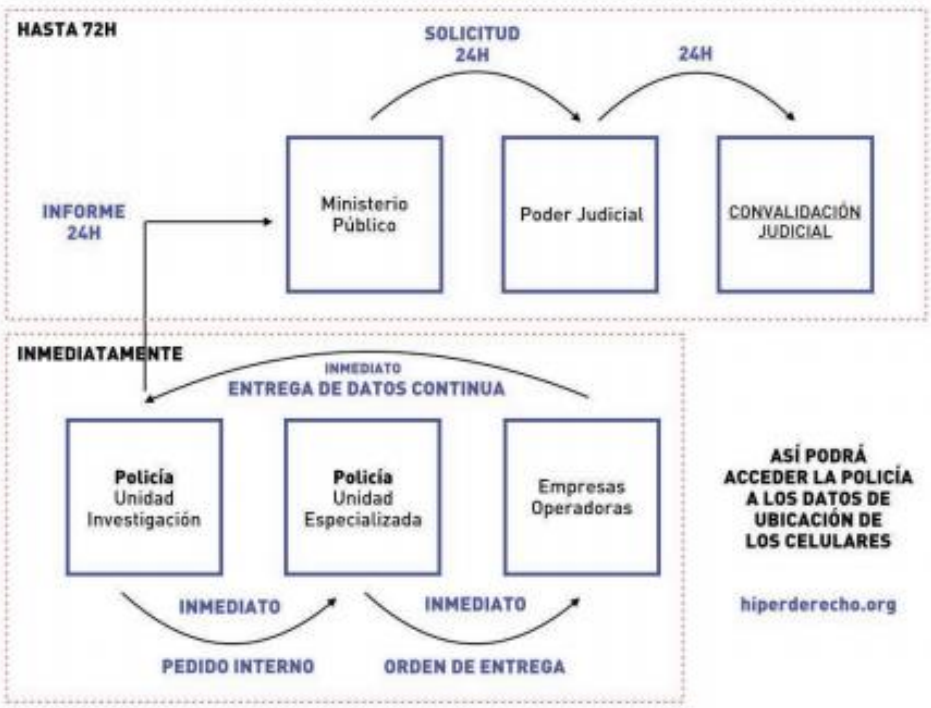
Público en el ámbito de su función." En consecuencia, pese a que la norma no lo expresa, si el Fiscal no está de acuerdo con la solicitud de la Policía tiene toda la potestad de ordenar se deje sin efecto la medida. ***El problema surgirá cuando la Policía haya obtenido información relacionada a la localización o geolocalización y después la Fiscalía muestre su disconformidad con tal pedido: ¿qué sucede con la información?, ¿quién se responsabilizará por la lesión sufrida por el ciudadano afectado? Al no contar con el Protocolo de actuación (porque el Ejecutivo le ha conferido la condición de información reservada) no sabemos de qué forma la Fiscalía comunicaría la revocatoria de la solicitud policial a la operadora de telefonía: ¿directamente?, ¿a través de la Unidad Especializada de la Policía?, ¿a través de la Unidad de Investigación?*** (Elías. R, 2016)

vi. ***El juez competente resolverá mediante trámite reservado y de manera inmediata, teniendo a la vista los recaudos del requerimiento fiscal, en un plazo no mayor de 24 horas. La denegación del requerimiento deja sin efecto la medida y podrá ser apelada por el Fiscal. El recurso ante el juez superior se resolverá en el mismo plazo y sin trámite alguno (artículo 5.3). El juez que convalida la medida establecerá un plazo máximo que no excederá de sesenta (60) días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del Fiscal (artículo 5.4).***

Este último paso debió ser el segundo en el procedimiento –el primero, obviamente, sería la comunicación y solicitud a cargo del Fiscal–. Ya que toda norma es perfectible, consideramos que, en una eventual reforma, debería establecerse, al igual que en artículo 230 del Código Procesal Penal,

que la resolución judicial debería indicar la información a la cual la Fiscalía puede acceder. Esto impedirá que la convalidación judicial sea tomada como un “cheque en blanco” que autoriza cualquier solicitud de información relacionada a la localización. Sin esta precisión, la Fiscalía o la Policía podrían solicitar ubicaciones históricas que no se encuentran vinculadas a la investigación criminal y, de este modo, lesionar el derecho a la intimidad personal. (Elías. R, 2016)

El siguiente flujograma explica gráficamente los pasos que, de acuerdo al Decreto Legislativo, sigue la Policía para acceder a nuestra localización o geolocalización. (Elías. R, 2016)



¿Qué pasa si la persona afectada acude directamente al Ministerio Público a denunciar, por ejemplo, una extorsión telefónica? Al no encontrarse acreditada o regulada normativamente, ¿la Fiscalía debería derivar el caso a la Unidad de

Investigación Policial para que solicite, a su vez, que la Unidad Especializada de la Policía requiera a las empresas operadoras la ubicación del dispositivo electrónico?

Si esto es así, el procedimiento estaría siendo monopolizado por el Ejecutivo, a través de la Policía, desplazando a su vez al titular natural de la acción penal. (Elías. R, 2016)

b) El decreto Legislativo genera confusión de roles entre la Policía y el Ministerio Público.

De acuerdo al artículo IV del Código Procesal Penal, el Ministerio Público es el titular del ejercicio público de la acción penal y el encargado de conducir la investigación criminal desde el inicio. En consecuencia, "conduce y controla jurídicamente los actos de investigación que realiza la Policía Nacional." el Decreto Legislativo fue diseñado para que el pedido de información relacionado a la localización y geolocalización estuviese en control y monopolio del Poder Ejecutivo, a través de la Policía Nacional.

Un problema adicional que el Decreto Legislativo genera es la confusión de roles en la investigación criminal. Así, un logro obtenido con el Código Procesal Penal fue circunscribir las funciones de la Policía al plano operativo / forense y las funciones de la Fiscalía al plano jurídico.

Antes de la promulgación del referido Código, por ejemplo, ***la Policía tenía la facultad de calificar jurídicamente los hechos investigados bajo las figuras de atestado policial y parte policial.*** El primero se refiere a la calificación jurídica y atribución de responsabilidad al investigado, mientras que la segunda al reconocimiento contrario, es decir, a la falta de responsabilidad. (Elías. R, 2016)

Se sostiene que el Decreto Legislativo renueva esta confusión al exigir que sea el Policía y no el Fiscal quien valore jurídicamente si nos encontramos ante un supuesto de flagrancia de cualquier delito que sea sancionado con más de cuatro años en el Código Penal (el Ejecutivo no incorporó una lista taxativa de aplicación, sino empleó una fórmula general que no distingue entre tipos de delitos).

Hay que recordar que en el artículo 230 del Código Procesal Penal regula la intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles. Así, el numeral 4 de la norma en referencia precisa que:

> Los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento. Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento. (Elías. R, 2016)

Por último, como puede apreciarse, un mismo supuesto de hecho (el acceso a la geolocalización de teléfonos móviles) ahora reviste dos mecanismos procesales: uno constitucional –exige resolución judicial previa– y uno inconstitucional –permite el acceso sin resolución judicial previa–, la flagrancia no valida el empleo del Decreto Legislativo

Entre los riesgos de la geolocalización se encuentran: "los seguimientos-trazabilidad de todo tipo de entidades (personas, animales, objetos), generación clandestina de perfiles-patrones (donde te encuentras, por donde te mueves, qué visitas, con quién te encuentras, cuánto tiempo estás, qué actividades haces, etc. vulnerando cuestiones relacionadas con la raza, política, religión, sexo, salud, etc.)

para luego aplicarlos con herramientas de minería de datos (…) El geotagging permite conocer y señalar las coordenadas donde se encuentra una persona, casa (para robarla), se tomó una foto, bailamos, nos divertimos, hicimos negocios, restaurante, un lugar secreto, la localización de un evento, etc. pero como riesgo nos encontramos con la vigilancia social por GPS y la posibilidad que nos establezcan patrones de nuestros movimientos. Como contramedida sencilla frente al geotagging inhabilitar en el Smartphone o cámara de fotos (ya sea Android, iPhone o Blackberry) dicha característica que está activada por defecto"

2.3.3. Derechos constitucionales vulnerados.

El Decreto Legislativo N° 1182 es un instrumento de vigilancia estatal masiva que viola la privacidad; la intimidad el secreto de las comunicaciones y la protección de datos personales de todos los peruanos, al hacer de libre disposición policial la información sobre ubicación y desplazamiento de cualquier persona.

También convierte a nuestros teléfonos celulares y computadoras en aparatos de monitoreo de nuestras comunicaciones, hábitos y desplazamientos.

2.3.3.1. Derecho a la Intimidad.

La intimidad es un derecho humano fundamental y es cardinal para el mantenimiento de sociedades democráticas. Es esencial a la dignidad humana y refuerza otros derechos, tales como la libertad de expresión y de información, y la libertad de asociación. Además, es reconocida por el derecho internacional de los derechos humano (INFODF, 2015)

La Vigilancia de las Comunicaciones interfiere con el derecho a la intimidad entre varios otros derechos humanos. Como resultado, sólo puede estar justificada

cuando es prescrita por ley, es necesaria para lograr un objetivo legítimo, y es proporcional al objetivo perseguido. (INFODF, 2015)

Antes de la adopción pública de Internet, principios jurídicos bien definidos y cargas logísticas inherentes al monitoreo de las comunicaciones crearon límites a la Vigilancia de las Comunicaciones por el Estado. En décadas recientes, esas barreras logísticas a la vigilancia han disminuido y ha perdido claridad la aplicación de principios jurídicos en los nuevos contextos tecnológicos. La explosión del contenido digital en las comunicaciones y de la información acerca de ellas, el costo cada vez menor de almacenamiento y la minería de grandes cantidades de datos, y el suministro de contenido personal a través de proveedores de servicios externos, hacen posible llevar la Vigilancia de las Comunicaciones estatal a una escala sin precedentes. (INFODF, 2015)

Mientras tanto, las conceptualizaciones de la legislación vigente en materia de derechos humanos no han seguido el ritmo de las modernas y cambiantes tecnologías y técnicas estatales de Vigilancia de Comunicaciones, la habilidad del Estado para combinar y organizar la información obtenida mediante distintas técnicas y tecnologías de vigilancia, o la creciente susceptibilidad de la información a la que se puede acceder. (INFODF, 2015)

La frecuencia con la que los Estados procuran acceder tanto al contenido de las comunicaciones como a los metadatos de las comunicaciones aumenta drásticamente, sin controles adecuados. (INFODF, 2015)

Los metadatos de las comunicaciones pueden crear un perfil de la vida de un individuo, incluyendo condiciones médicas, puntos de vista políticos y religiosos, asociaciones, interacciones e intereses, revelando tan o, incluso, más

detalladamente de lo que sería posible desde el contenido de las comunicaciones. (INFODF, 2015)

A pesar del gran potencial para la intromisión en vida del individuo y el efecto negativo sobre las asociaciones políticas y otras, las leyes, normas, poderes o autoridades a menudo ofrecen a los metadatos de las comunicaciones un menor nivel de protección y no ponen restricciones suficientes sobre cómo pueden ser posteriormente utilizado por los Estados. (INFODF, 2015)

2.3.3.2. Derecho a la Privacidad.

El derecho a la privacidad es "El derecho de la persona a ser protegida de la intromisión en su vida o asuntos personales o aquellos de la familia, por medios físicos directos o por medio de la publicación de informaciones". (Privacy International, 2015).

El derecho a la privacidad es aquel encargado en proteger de manera psicológica y física a cada persona, de intromisiones no queridas o deseadas, efectuadas por terceros. Este derecho debe tutelar ciertos factores de las personas, como la libertad para sentirse libre de realizar acciones que generan distintas experiencias. (Omeba, E, 2005).

El derecho a la privacidad se vislumbró desde el momento en que surgió la inquietud por preservar la intimidad de las personas y la conciencia por otorgarles esa facultad. Este derecho puede definirse como aquel que los individuos poseen para separar aspectos de su vida íntima del escrutinio público, por lo que, sin distinción, todos tenemos derecho a ella.

2.3.3.3. Derecho al Secreto de las Comunicaciones.

Según el inciso 10 del artículo 2 de la Constitución Política del Perú, el secreto de las telecomunicaciones es un derecho de rango constitucional. Asimismo, no debe perderse de vista el artículo 16 del Código Civil, que regula la confidencialidad de la correspondencia y demás comunicaciones. Adicionalmente, en el artículo 4 del Texto Único Ordenado de la Ley de Telecomunicaciones (aprobado mediante Decreto Supremo N° 013-93-TCC), el artículo 13 de su Reglamento (aprobado mediante Decreto Supremo N° 020-2007-MTC) y la Resolución Ministerial N.º 111-2009-MTC/03, se contempla el derecho a la inviolabilidad y el secreto de las telecomunicaciones, y la protección de datos personales de los abonados y usuarios (Chipana, J & López J, 2019).

Cabe señalar también que estos derechos están protegidos en los contratos de concesión celebrados por las operadoras del servicio público de telecomunicaciones con el Estado peruano. (Chipana, J & López J, 2019)

De esta forma, existe un derecho consagrado en nuestra Constitución, el mismo que ha sido desarrollado y delineado en normas infraconstitucionales. (Chipana, J & López J, 2019)

Así, en el ámbito constitucional: “La protección que se da es del secreto y la inviolabilidad. Por secreto se debe entender que el contenido de las comunicaciones o de los papeles privados de una persona sólo puede ser conocido por ella y aquélla o aquéllas otras con las cuales deseó comunicarse. Hay que notar que el secreto de una comunicación de dos personas pertenece a las dos y exclusivamente a ellas. (Chipana, J & López J, 2019)

En otras palabras, las dos tienen derecho a saber el contenido de la comunicación y sólo pueden transmitirlo a terceros con mutuo acuerdo. Si sólo uno de ellos hiciera de conocimiento de otros el contenido de la comunicación, en realidad estaría violando el secreto de su contraparte. (Chipana, J & López J, 2019)

La inviolabilidad consiste en que las comunicaciones no pueden ser intervenidas, esto es, las cartas interceptadas, las ondas electromagnéticas estorbadas con transmisiones que las hagan inútiles para la comunicación, los teléfonos intervenidos, etc. La inviolabilidad no tiene que ver con el contenido, sino con el proceso mismo de la comunicación o con la sustracción de los documentos privados". (Rubio, C, 1999)

En ese sentido, es claro que existe una obligación de reserva, tanto del secreto de las telecomunicaciones, como de la información personal los usuarios, la misma que sólo puede ser levantada en los casos donde exista:

- Un mandato judicial específico y motivado; o,
- El consentimiento previo, expreso y por escrito del titular. Por lo tanto, el secreto a las telecomunicaciones no es un derecho de carácter absoluto, sino que el mismo puede ser levantado por un mandato judicial o a solicitud de parte. (Chipana, J & López J, 2019)

De esta forma, debe entenderse que el contenido del derecho a la protección del secreto de las telecomunicaciones no sólo alcanza al contenido de la comunicación en sí, sino también comprende los registros de las comunicaciones

que pueden incluir datos como el origen, el destino, la fecha, la duración, entre otros (Chipana, J & López J, 2019).

Estos registros también se conocen como Calling Data Records (o, su abreviatura, CDR). En esa línea, se puede inferir que el derecho al secreto de las telecomunicaciones incluye el contenido de la comunicación, el registro del dispositivo a través del cual se realiza, la identificación de la identidad de las partes en la comunicación y cualquier otra información que provenga como resultado de este proceso. Para conocer toda esta información, será fundamental la intervención de un perito (Chipana, J & López J, 2019)

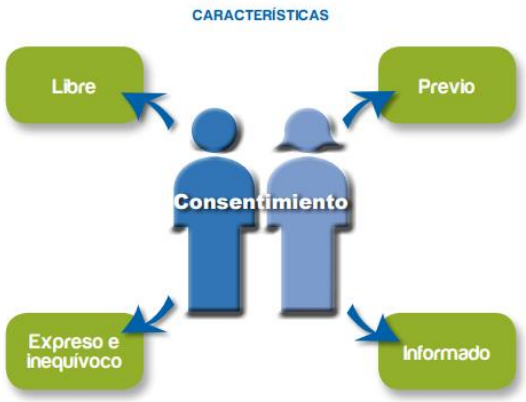
Por otro lado, especial atención merece el tema del acceso a la información histórica de las comunicaciones, que es el procedimiento más antiguo relacionado al levantamiento del secreto de las telecomunicaciones, debido a que hace algunos años no existían protocolos técnicos regulares que permitían a la policía una interceptación en tiempo real. (Chipana, J & López J, 2019)

Ahora bien, el acceso a la información en tiempo real se comenzó a regular con el Decreto Legislativo N° 1182 publicado en el año 2015. En él se establece el procedimiento para el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado. (Chipana, J & López J, 2019).

2.3.3.4. Derecho a la Protección de Datos personales.

Para el tratamiento de los datos personales se necesita el consentimiento del titular del dato personal. Solo en casos muy concretos, la ley puede autorizar lo contrario.

Gráfico N° 4. Características.



Fuente: Fuente especificada no válida.

El derecho fundamental a la protección de datos persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado.

El objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales.

El Derecho a la protección de datos atribuye un haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo

es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho de acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales.

2.3.4. Derecho Penal.

2.3.4.1. Delitos Flagrantes de conformidad con lo dispuesto en el artículo 259 del Código Procesal Penal.

La palabra flagrante viene del latín flagrans - flagrantis, participio de presente del verbo flagrare, que significa arder o quemar, y se refiere a aquello que está ardiendo o resplandeciendo como fuego o llama, y en este sentido ha pasado a nuestros días, de modo que por delito flagrante en el concepto usual hay que entender aquel que se está cometiendo de manera singularmente ostentosa o escandalosa.

El artículo 259 del CPP señala: la Policía Nacional del Perú detiene, sin mandato judicial, a quien sorprenda en flagrante delito, existe flagrancia cuando:

1. El agente es descubierto en la realización del hecho punible.

2.El agente acaba de cometer el hecho punible y es descubierto.

3. El agente ha huido y ha sido identificado durante o inmediatamente después de la perpetración del hecho punible, sea por el agraviado o por otra persona que haya presenciado el hecho, o por medio audiovisual, dispositivos o equipos con cuya tecnología se haya registrado su imagen, y es encontrado dentro de las veinticuatro (24) horas de producido el hecho punible.

4. El agente es encontrado dentro de las veinticuatro (24) horas después de la perpetración del delito con efectos o instrumentos procedentes de aquel o que

hubieren sido empleados para cometerlo o con señales en sí mismo o en su vestido que indiquen su probable autoría o participación en el hecho delictuoso

En ninguno de los supuestos antes citado, se señala sobre flagrancia a futuro ya que la norma no dice el agente que será descubierto, el agente va a cometer y es necesario su descubrimiento, el agente podría o será encontrado; sin embargo en la praxis se utiliza mal la nomenclatura de flagrancia no está ni siquiera calza en ningún supuesto con el caso en concreto planteado, en consecuencia la Policía Nacional del Perú no tiene ninguna autoridad para intervenir frente a un hecho que tiene conocimiento sin intervención del representante del Ministerio Público.

2.3.4.2. Clasificación de la Flagrancia Delictiva.

2.3.4.2.1. Flagrancia estricta o propiamente dicha. Con las manos en la masa.

- Que, en primer lugar, el agente in fraganti es el delincuente sorprendido cuando está realizando actos de ejecución propios del delito, o cuando acaba de consumarlo.

- El requisito de sorprender al delincuente no exige el asombro o sobresalto del mismo, se trata de que sea descubierto, su acción delictiva en fase de ejecución o inmediatamente después de la misma. El descubrimiento ha de producirse precisamente mediante la percepción sensorial del hecho, por parte del sujeto que dispone la detención, es decir, este ha de tener conocimiento del hecho a través de sus sentidos, normalmente la vista.

- La percepción que se realiza es absolutamente actual, directa y efectiva y no tiene que efectuarse ninguna deducción. Es decir, el hecho advertido resulta vivo y palpitante. (López, J, 2015)

2.3.4.2.2. Cuasiflagrancia.

Se da este supuesto cuando ya se ha ejecutado el delito, pero es detenido poco después, ya que no se le perdió de vista desde entonces.

En otras palabras, una persona puede ser detenida aun después que ejecuto o consumo la conducta delictiva, pero siempre y cuando no le hayan perdido de vista y sea perseguido desde la realización del hecho delictivo. (López, J, 2015)

Por ejemplo: *Un miembro policial percibe que se está cometiendo un delito y el agente activo se percata de ello y decide fugarse. En este caso, el efectivo policial lo persigue por un lapso corto de tiempo y logra su captura, en este ejemplo el efectivo policial ha percibido en forma directa la comisión del ilícito penal. Tenemos presente: La inmediatez personal, temporal y la situación de descubrimiento. Este tipo de flagrancia se apoya en una deducción lógica a partir de indicios muy poderosos.* (López, J, 2015)

2.3.4.2.3. Flagrancia por identificación inmediata.

Tiene como base que el agente ha sido identificado como autor del hecho. Se configura cuando el agente ha huido y ha sido identificado durante o inmediatamente después de la perpetración del hecho punible, sea por el agraviado o por otra persona que haya presenciado el hecho, o por medio audiovisual, dispositivos o equipos cuya tecnología se haya registrado su imagen, y es encontrado dentro de las 24 horas de producido el hecho punible.

No habría inmediatez temporal y personal. Pero hay evidencia fuerte de su autoría. Esta fórmula constituye una presunción de flagrancia en atención a la identificación del agente, lo cual exige una investigación rápida y de resultado por parte de la policía. (López, J, 2015)

2.3.4.2.4. Presunción de flagrancia. Por evidencias o inferida.

Por citar un ejemplo en la flagrancia presunta el agente activo fuga del lugar después de haber cometido un ilícito. Luego un efectivo policial toma conocimiento del hecho delictivo y, justamente, observa a una persona con elementos que posiblemente lo vinculan con el ilícito conocido y lo interviene. (López, J, 2015)

Para que se dé la presunta flagrancia se requiere una mínima investigación y ello es función y competencia de la Policía Nacional. La tesis que vincula al intervenido como presunto autor, surge de inmediato y prácticamente entera; los elementos de convicción de cargo aparecen palpitantes, objetivos, concurrentes, fuertes, lógicos, verosímiles, con capacidad de generar firmes convicciones y hasta certezas, de tal modo que generan la urgencia de actuar deteniendo al autor. (López, J, 2015)

2.3.4.3. Cuando la investigación del delito sea sancionada con pena superior a los cuatro años de pena privativa de libertad.

El comportamiento típico, antijurídico y culpable que protagoniza un cuidado activa el sistema penal oponiendo al autor una determinada consecuencia jurídica. Siendo las consecuencias jurídicas son las penas, las medidas de seguridad, las

medidas accesorias y las responsabilidades civiles que derivan del delito. (Marcia, R, 2013)

La característica formal del Derecho consiste en que puede ser impuesto de modo inexorable a todos los sujetos, a cualquier precio, con, sin o en contra de la voluntad de estos, venciendo en tal caso su resistencia por medio de la fuerza. La pena es una manifestación de la impositividad inexorable del derecho. (Marcia, R, 2013)

El iuspuniendi es la facultad de imponer el cumplimiento de penas o medidas de seguridad a las personas que realizan comportamientos prohibidos en la ley penal.

Es un derecho subjetivo del Estado que surge de la relación jurídica entre el Estado y el que infringe la ley penal (imputado) en virtud de la cual uno tiene derecho a imponer una pena o medida y aquél a sufrirla. (Marcia, R, 2013)

Por otro lado, el derecho penal es la última ratio que tiene una sociedad para reaccionar contra aquellos comportamientos que lesionan o ponen en peligro un bien jurídico, al ser ultima ratio la sanción penal ha de ser usada únicamente después que los otros mecanismos de control social han fracasado. Es decir, las normas penales han de ser subsidiarias a las demás.

En este sentido, el derecho penal responde a la política criminal diseñada en la Constitución de un determinado Estado, política que tiene en la familia, la escuela y las demás ramas del derecho otros mecanismos para controlar la existencia de comportamientos socialmente desestabilizadores. (Marcia, R, 2013)

2.3.4.3.1. Principios del derecho penal limitadores.

El derecho penal se rige por estrictos principios limitadores del ius puniendi, con límites cuantitativos (con relación al número de tipos penales que debe dictar un legislador en la actualidad y a la forma de aplicar las penas), así como límites cualitativos (la intervención estatal debe hacerse en la forma señalada en la constitución y las leyes) (Marcia, R, 2013)

Mediante los límites cuantitativos se debe optar por las penas menos gravosas, que sean suficientes para restablecer el ordenamiento jurídico transgredido, debe haber una proporcionalidad entre el delito cometido y la pena, la duración de la pena debe estar prefijada dentro de ciertos límites, en la forma previa y por la ley, además sólo se pueden tipificar conductas que atentan contra valores fundamentales denominados “bienes jurídicos penalmente protegidos. (Marcia, R, 2013)

Los límites cualitativos se refieren que se realizan bajo la dirección de ciertos principios:

- Principio de legalidad o intervención legalizada;
- Intervención mínima;
- Principio de legalidad en lo referido al iuspuniendi (las penas a imponer a causa de la comisión de un delito sólo pueden ser establecidas y determinadas en su duración por el legislador, al juez toca sólo determinarlas para el caso concreto, pero siempre del marco legal pre fijado);

- Principio de intervención mínima. El derecho penal precisa las sanciones, qué deben consistir las penas o las medidas de seguridad, estableciendo su índole, su intensidad y propósito de cara a la sociedad y al orden jurídico. (Marcia, R, 2013)

El derecho penal moderno ha humanizado sus penas, desapareciendo con ello la afectación de la integridad corporal (torturas, azotes, mutilaciones), o las penas infrahumanas como la de la picota (el rollo) del sentenciado, y ha reemplazando este tipo de penas, por la de privación de la libertad personal, para delitos graves y fórmulas alternativas de punición a la privación de la libertad, como multas u otras privativas de variados derechos, para delitos menores o faltas". (Marcia, R, 2013)

En el derecho penal moderno, existe una reserva del uso legítimo de la violencia en los poderes públicos, ya que el Estado es el único que utiliza las penas como un medio de control social legítimo.

Es un instrumento de control formalizado que debe ser aplicado a la persona en forma proporcional y legal. (Marcia, R, 2013)

2.3.4.3.2. Pena Privativa de Libertad.

La pena privativa de libertad impone al condenado la obligación de permanecer encerrado en un establecimiento. El penado pierde su libertad ambulatoria por un tiempo de duración variable que va de la mínima de dos días hasta la cadena perpetua (Art. 29 del C. P.) (Marcia, R, 2013)

2.3.4.4. Cuando el acceso a los datos constituya un medio necesario para la investigación.

La norma otorga facultades directas a la unidad especializada de la Policía Nacional para acceder de forma inmediata a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar, cuando constituya un medio necesario para la investigación, en los casos de flagrancia previsto en el artículo 259 del Código Procesal Penal.

2.3.4.4.1. Datos de Investigación.

En términos generales, podemos decir que los datos de investigación son datos que son recolectados, observados o creados para ser analizados y producir resultados de investigación originales. Sin embargo, es importante tener en cuenta que no existe una única definición, y que diferentes disciplinas o comunidades pueden diferir en su entendimiento de este concepto.

Así, puede haber grandes diferencias entre lo que constituye un dato para investigadores de la humanidad, de las artes o de las ciencias. En cualquiera de estos casos, es importante tener en cuenta que los datos pueden ser de tipo cuantitativo o cualitativo, y que pueden venir en muchos formatos y soportes, ya sean físicos o digitales.

2.3.4.4.2. Tipos de datos.

- *Datos primarios o sin procesar:* Datos originales que han sido recolectados, pero aún no han sido procesados o analizados. Algunos ejemplos son los registros sonoros, observaciones, notas de campo o datos de experimentos.

- Datos procesados: Datos que han sido digitalizados, traducidos, transcritos, limpiados, validados, verificados y/o anonimizados.

- *Datos analizados:* Modelos, gráficos, tablas, textos u otros, que han sido creados a partir de los datos primarios y procesados, y que se pretende sean de ayuda en el descubrimiento de información útil, la presentación de conclusiones y la toma de decisiones.

2.3.5. Derecho Comparado.

En algunos países se han creado estratégicamente leyes para proteger y tratar a los datos personales. Estas leyes se adecúan a las necesidades de cada uno de sus países. Para que no existan falencias jurídicas, como vacíos legales o falta de normativa, siendo que al no existir un adecuado amparo se genera perjuicios a sus ciudadanos.

En la actualidad, se vive en una sociedad informatizada, utilizando el avance tecnológico, logrando eliminar las barreras, como la distancia o el tiempo, y facilitando la obtención de datos. En consecuencia, ya no es necesario la fuerza física, para influir o controlar a las personas, ya que se hace por medio de uso de la información. Al evitar medios coactivos, para el manejo de la conducta de los ciudadanos, utilizando los datos, se ha facilitado el manejo adecuado de preciso de los sujetos.

El siguiente proyecto se realizará una comparación respecto a las normas que regulan La Protección a los Derechos Constitucionales; entre ellos los países a considerar son los siguientes:

2.3.5.1. México.

Regula la relación entre los sujetos obligados y los titulares de la información, regulando de tal forma la transparencia y remisión de datos, utilizando acciones preventivas durante su proceso. Sancionando o impugnando a los procedimientos ilegales, para proceder a una verificación de estos. Establece las obligaciones y deberes de los sujetos obligados, los que a su vez pueden expedir, tramitar o modificar normativa. (García. C y Enríquez)

2.3.5.2. Colombia.

El ente regulador encargado de la protección de la información, es el Registro Nacional de Bases de Datos, conocido como RNBD. Este es el directorio Público, que se encarga de que los sujetos administradores de dichas bases de datos tengan el control y manejo adecuado sobre estos.

El Gobierno en el Decreto Único 1074 de 2015 (Decreto 886 de 2014 Art 3), impartió la obligación a todos los responsables de tratamientos de datos Empresas y personas naturales, de inscribir las bases de datos que se manejen, en la plataforma de Registro Nacional de Base de Datos RNBD que es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el ente encargado de administrar y sancionar frente al manejo de datos y su registro es la Superintendencia de Industria y Comercio.

Si bien para los Empresarios o quien maneja datos sea persona natural o jurídica (ley 1581 de 2012 protección de datos personales), su mayor preocupación ha sido basarse en el riesgo del no registro de estas bases de datos que trae como consecuencia sanciones, las cuales se desconocen su aplicación, y que requieren de

criterios objetivos y subjetivos sometidos a una graduación con base a unos criterios establecidos por la ley 1581 de 2012 en su artículo 23.

2.3.5.3. Paraguay.

Regulado por el Proyecto de Ley de Retención de Datos o Ley Pyrawebs (2014) Obliga a los proveedores de servicios de Internet a conservar los datos de tráfico de sus usuarios por doce meses, con el fin de poder ser accedidos por un juzgado competente.

El proyecto de ley, bautizado "PYRAWEBS", parece perseguir un fin perfectamente legítimo en una sociedad democrática: prevenir y sancionar hechos criminales punibles que se cometen a través de Internet. Pero la legitimidad de la medida no se consume en la pregunta respecto de su fin, sino que debe analizarse la forma en la que este pretende cumplirse. En el caso del proyecto, que se refiere expresamente a hechos tipificados en el Código Penal Paraguayo además de "otras leyes penales especiales", no hay mención alguna a las garantías exigibles para evitar abusos y cuenta con escasos contrapesos.

El proyecto de ley parece explicitar que la norma de retención de datos se refiere solamente a los "metadatos" y no a los contenidos, específicamente a los datos de tráfico: dirección IP, origen y destino de la comunicación, hora y fecha de conexión y desconexión, itinerario, tamaño y duración de la comunicación. Pero esta distinción, promovida por buena parte de aquellos organismos de persecución criminal, en la práctica, es bastante más gris de lo que parece.

Las agendas y las direcciones de email con quienes intercambiamos correos de manera frecuente e incluso nuestro historial de navegación, calificados como

meros “metadatos”, son suficientemente ilustrativos a la hora de identificar una persona o hacerla identificable.

Ejemplo: Si se analiza los metadatos de una llamada al ginecólogo realizada por una joven mujer que luego llama a su madre, luego a un hombre con quien se ha comunicado repetidamente en los últimos meses y luego a una clínica de abortos, probablemente podemos deducir bastante más que lo que podríamos conseguir de una conversación con ella. En resumen, no hay buenas razones para argumentar que los “metadatos” merecen una protección más débil que el contenido mismo de las comunicaciones.

2.3.5.4. Argentina.

Ley Nacional de Telecomunicaciones (1972) y Ley de Protección de datos personales (2000).

- *Ley Nacional de Telecomunicaciones.*

  - ✓ *Telecomunicación:* Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

  - ✓ *Radiocomunicación:* Toda telecomunicación transmitida por medio de las ondas radioeléctricas.

  - ✓ *Telegrafía:* Sistema de telecomunicación que permite obtener una transmisión y reproducción a distancia del contenido de documentos tales como escritos, impresos o imágenes fijas o la reproducción a distancia en

esa forma de cualquier información.

- ✓ *Telefonía:* Sistema de telecomunicación para la transmisión de la palabra o, en algunos casos, de otros sonidos.

- ✓ *Servicio de Radiodifusión:* Servicio de radiocomunicación cuyas emisiones se destinan a ser recibidas directamente por el público en general. Dicho servicio abarca emisiones sonoras, de televisión o de otro género.

- ✓ *Servicio telefónico:* Servicio que permite a sus usuarios comunicarse directa o temporalmente entre sí, por medio de aparatos telefónicos y circuitos de la red telefónica pública.

- ✓ *Servicio telegráfico público:* Servicio que asegura la aceptación y remisión de despachos y telegramas con brevedad y a corta o larga distancia a través de los telégrafos.

- ✓ *Servicio télex:* Servicio telegráfico que permite a sus usuarios comunicarse directa o temporalmente entre sí por medio de aparatos arrítmicos y circuitos de la red telegráfica pública.

- ✓ *Servicio de radioaficionados:* Servicio de instrucción individual, de intercomunicación y de estudios técnicos efectuado por aficionados, esto es por personas debidamente autorizadas que se interesan en la radiotécnica con carácter exclusivamente personal y sin fines de lucro.

- ✓ *Servicio espacial:* Servicio de radiocomunicación entre estaciones terrestres y estaciones espaciales, o entre estaciones espaciales, o entre estaciones terrenas cuando las señales son retransmitidas por estaciones

espaciales o transmitidas por reflexión en objetos situados en el espacio, excluyendo la reflexión o dispersión en la ionósfera o dentro de la atmósfera de la Tierra.

- ✓ *Servicio especial:* Servicio de telecomunicación no definido en forma específica en otra parte de la presente ley o su reglamentación destinado a satisfacer determinadas necesidades de interés general y no abierto a la correspondencia pública.

- ✓ *Servicio limitado:* Servicio de telecomunicación ejecutado por estaciones no abiertas a la correspondencia pública y que está destinado al uso exclusivo de personas físicas o jurídicas determinadas.

- ✓ *Servicio interno*: Servicio de telecomunicación entre oficinas o estaciones de telecomunicación de cualquier naturaleza, que se hallen dentro del territorio de la Nación y en los lugares sometidos a su jurisdicción.

- ✓ *Servicio internacional*: Servicio de telecomunicación entre oficinas o estaciones de cualquier naturaleza del servicio interno con las de otros países.

- ✓ *Correspondencia de telecomunicaciones:* Toda comunicación que se efectúe por los medios de telecomunicaciones públicos o privados autorizados.

- ✓ *Sistema nacional de telecomunicaciones:* Es el conjunto de estaciones y redes de telecomunicaciones integradas, alámbricas o inalámbricas abierto a la correspondencia pública para el tráfico interno e internacional.

- ✓ *T*odo vocablo o concepto no definido en esta ley, tiene el significado establecido en los convenios y reglamentos nacionales e internacionales.

- *La ley de protección de datos personales.* -

Tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. A los fines de la presente ley se entiende por:

- ✓ *Datos personales:* Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

- ✓ *Datos sensibles:* Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

- ✓ *Archivo, registro, base o banco de datos:* Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

- ✓ *Tratamiento de datos:* Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de

datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

- ✓ *Responsable de archivo, registro, base o banco de datos:* Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

- ✓ *Datos informatizados:* Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

- ✓ *Titular de los datos:* Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

- ✓ *Usuario de datos:* Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.

- ✓ *Disociación de datos:* Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

2.3.5.5. Unión Europea.

Directiva de Retención de Datos (2006); sobre la conservación de datos tratados o generados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y, a la conservación de datos de comunicación en relación con el acceso a Internet, la telefonía por Internet y el correo electrónico por Internet.

2.4. Marco Conceptual.

2.4.1. Problemas que surgen de la geolocalización.

La geolocalización consiste en obtener la ubicación geográfica de un objeto como puede ser un teléfono móvil, Tablet, dispositivo que esté conectado a una red. Para ello se puede utilizar diferentes métodos como por ejemplo comprobar el código postal de una carta, la dirección IP de un equipo o el sistema GPS de nuestro teléfono móvil.

Para obtener la ubicación geográfica aproximada de un smartphone se utiliza un sistema de posicionamiento global. El sistema está formado por una red de satélites geoestacionarios que dan cobertura a toda la Tierra. Para obtener la ubicación el dispositivo se conecta como mínimo con 3 satélites, de estos satélites recibe un identificador y la hora de cada uno ellos. El dispositivo calcula el tiempo que tarda en llegar la señal desde los satélites y gracias al retardo o de la resultante se obtiene la ubicación por medio de la triangulación.

2.4.1.1. La Inconstitucionalidad de la ley de geolocalización.

El Decreto Legislativo N° 1182, publicado el 27 de julio de 2015, regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación en la llamada "lucha contra la delincuencia y el crimen organizado". también conocida como la Ley Stalker.

En esencia, dicha norma otorga facultades directas a la unidad especializada de la Policía Nacional para acceder de forma inmediata a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza

similar, cuando constituya un medio necesario para la investigación, en los casos de flagrancia previsto en el artículo 259 del Código Procesal Penal y cuando se trate de delitos sancionados con pena privativa de libertad que supere los cuatros años.

El único mecanismo establecido para el control ex post de dicha medida, se sustenta en la convalidación judicial.

La norma señala que, dentro de las 24 horas de haberse obtenido los datos de localización o geolocalización, la unidad a cargo de la investigación policial deberá remitir a la Fiscalía un informe que sustente el requerimiento para su convalidación judicial, ante la cual la Fiscalía debe solicitar al Juez la convalidación de la medida, quien podrá denegar la convalidación o convalidar la misma.

El procedimiento policial establecido para el acceso a los datos de localización y geo localización es directo y automático, es decir, no se exige requerimiento Fiscal ni orden judicial previa a la obtención de dichos datos.

Las empresas concesionarias de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, están obligadas a brindar a la Policía Nacional los datos de localización o geolocalización de manera inmediata, sin exigir orden judicial, requerimiento fiscal, o motivación suficiente, es decir deberán entregar la información de forma automática, sin siquiera tener facultades para verificar que se trate de un requerimiento policial debidamente motivado.

Pese a que la norma, señala que se debe excluir de este procedimiento a cualquier tipo de intervención de las comunicaciones, dicha afirmación no es clara

y más bien es contradictoria y ambigua, si tenemos en cuenta que para el uso de los datos derivados de las telecomunicaciones precisamente lo que se requiere realizar es una intervención en los dispositivos de comunicaciones.

En tal sentido, el hecho de intervenir comunicaciones para usar datos derivados de estos para la identificación, localización o geolocalización de otros equipos de comunicación, en sí representa una intervención en las comunicaciones de los titulares de los equipos, y dicha conducta se encuentra prohibida por abarcar el derecho constitucional al secreto e inviolabilidad de las comunicaciones y documentos privados previsto en el numeral 10 del artículo 2 de la Constitución, que expresamente señala que: "Las comunicaciones, telecomunicaciones o sus instrumentos solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley".

Adicionalmente, si bien la norma señala que este procedimiento se aplicará en los casos de flagrancia, y se trata de una intervención de los equipos, la norma no dice nada sobre los titulares de los equipos, quienes en realidad son los afectados directos con la intervención a sus equipos; y quienes por lo menos deberían tener la calidad de investigados para poder dictarse dicha medida contra sus equipos.

Por otro lado, el acceso a datos de localización y geolocalización sin orden judicial motivada no solo trae consigo la problemática con respecto al contenido del derecho al secreto de las comunicaciones y la reserva de los documentos privados, sino que también pone de manifiesto cuestiones referidas a la protección de derechos fundamentales tales como la inviolabilidad de la intimidad y la vida privada.

La afectación de dichos derechos constitucionales en la obtención de datos de localización y geolocalización sin orden judicial, traerá consigo la imposibilidad de valorar las pruebas obtenidas a partir de dichos datos por considerarse pruebas prohibidas al haber sido obtenidas con afectación a derechos fundamentales como la intimidad y la vida privada, lo que será aún más evidente en los casos que las convalidaciones solicitadas sean denegadas por el juez.

Finalmente, cabe destacar que en el art. 230 del Código Procesal Penal, que regula la "Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles", se considera como parte del contenido del derecho al secreto de las comunicaciones la intervención de las comunicaciones para la identificación, localización y geolocalización de equipos, tal es así que se exige que dicha intervención se realice previa orden judicial.

En ese sentido, específicamente en el inciso 4 se establece que: "Los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento.

Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento".

Es decir, la ley procesal establece dentro de los alcances de la medida de levantamiento de secreto de comunicaciones dictada por el juez, la obligación de

las empresas concesionarias de brindar la geolocalización de teléfonos móviles, e inclusive dicha norma es más clara porque establece que dicha medida podrá dictarse no solo contra el investigado sino también contra personas de las que cabe estimar fundadamente, en merito a datos objetivos determinados que reciben o tramitan por cuenta del investigado determinadas comunicaciones, o que el investigado utiliza su comunicación.

De esta forma, quedan en evidencia las ambigüedades, vacíos y contradicciones que trae consigo el Decreto Legislativo N° 1182, cuyo problema central radica en haberse otorgado facultades a la Policía para solicitar la intervención de comunicaciones para la identificación, localización y geolocalización de equipos, sin orden ni control judicial alguno.

Dicha norma prevé, entre otras cosas, dos mecanismos que permitirán acceder a la información privada de los ciudadanos, los cuales presentan serios cuestionamientos de constitucionalidad. A continuación, veremos las razones:

a) ¿Por qué revelar la geolocalización de una persona, sin mandato judicial, transgrede el secreto de las comunicaciones?

La norma faculta a la Policía Nacional, sin necesidad de intervención de un juez, a solicitar el acceso inmediato de los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar (llámese tablets, laptops, computadoras, etc.) de cualquier ciudadano. Estos datos suelen ser enviados de forma permanente por estos dispositivos, sean smartphones o teléfonos móviles tradicionales, lo cual permite registrar la circulación de sus usuarios.

Dicho requerimiento policial se efectuará a las empresas concesionarios de los servicios públicos de telecomunicaciones (Movistar, Claro, Entel, etc) o a las entidades públicas relacionadas con estos servicios, las cuales están obligados a brindar los datos de localización o geolocalización de manera inmediata, las 24 horas del día de los 365 días del año.

Para que este pedido sea válido, la Policía deberá verificar que se cumplan estos 3 presupuestos:

- Flagrancia delictiva,
- Que el delito investigado sea sancionado con pena superior a los 4 años, y
- Que el acceso a los datos constituya un medio necesario para la investigación. (La Ley, 2015)

Este procedimiento, por el cual se puede obtener la localización de un ciudadano través de los medios de comunicación sin mandato judicial, constituye una intervención desproporcionada en el derecho al secreto e inviolabilidad de las comunicaciones, protegido por el inc. 10 del artículo 2 de la Constitución. (La Ley, 2015)

Y es que si bien el artículo 6 de Decreto Legislativo N° 1182 declara que se excluyen los datos de localización o geolocalización del ámbito de protección del derecho al secreto e inviolabilidad de las comunicaciones, lo cierto es que con el avance tecnológico, las “comunicaciones” no solo abarcan las transacciones realizadas por medios electrónicos, sino que también comprende las interacciones o actividades productos de esta como la identidad de las partes, información de rastreo de ubicación incluyendo direcciones IP y otros. (La Ley, 2015)

A medida que avanzan las tecnologías que facilitan la vigilancia estatal de las comunicaciones, los Estados están fallando en garantizar que las leyes, normas, actividades, poderes (autoridades relacionadas con la Vigilancia de las Comunicaciones se adhieran a las normas y estándares internacionales de derechos humanos. (INFODF, 2015)

Asimismo, se busca clarificar cómo se aplica. el derecho internacional de los derechos humanos en el actual entorno digital, en particular a la luz del aumento y de los cambios que están teniendo las tecnologías y técnicas de Vigilancia de las Comunicaciones. (INFODF, 2015)

Así lo establecen los Principios Internacionales sobre la Aplicación de los derechos Humanos a la vigilancia de las Comunicaciones. El texto reafirma que la intimidad es un derecho fundamental y esencial para la dignidad humana y explica que la vigilancia de las comunicaciones constituye una injerencia con los derechos fundamentales. En ese sentido, las libertades fundamentales sólo pueden ser restringidas por ley. Además, toda restricción debe ser necesaria, idónea y proporcional para lograr un objetivo legítimo. (La Ley, 2015)

Estos principios pueden proporcionar a los grupos de la sociedad civil, a la industria y a los Estados un marco para evaluar si las leyes y prácticas de vigilancia, actuales o propuestas, están en línea con los derechos humanos.

Estos principios son el resultado de una consulta global con grupos de la sociedad civil, con la industria y expertos internacionales en legislación sobre Vigilancia de las Comunicaciones, políticas públicas y tecnología. (La Ley, 2015)

Cabe destacar que el Nuevo Código Procesal Penal también recoge esta figura, pero exige la previa autorización judicial. En efecto, en su artículo 230, dicha norma dispone que *"los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida".* Con ello, podemos reafirmar las contradicciones e irregularidades que trae consigo el decreto legislativo, al permitir a la Policía solicitar la localización de equipos sin control judicial. (La Ley, 2015)

b) *La retención de datos derivados de las comunicaciones violenta el derecho de la Privacidad.*

La norma prevé un segundo mecanismo de control en su segunda disposición complementaria final. Se establece que toda empresa que brinde servicios públicos de telecomunicaciones deberá guardar los datos derivados de las comunicaciones de cualquier persona hasta por 3 años. Así, se precisa que estas empresas deberán conservar estos datos durante los primeros 12 meses en sistemas informáticos que permitan su consulta y entrega en línea y en tiempo real, y por 24 meses adicionales en un sistema de almacenamiento electrónico. En este caso, la solicitud por parte de la Policía para que las empresas le entreguen estos datos sí necesitará de autorización judicial. El único mecanismo establecido para el control ex post de dicha medida, se sustenta en la convalidación judicial.

En nuestro país es la primera vez que se regula una norma expresa que apruebe la conservación de dichos datos hasta por 3 años que permitan al Estado su consulta o entrega inmediata. Pero, como podemos apreciar, el almacenamiento de esta información ha sido ya rechazada en la justicia internacional por violatoria de la privacidad de las personas. (La Ley, 2015)

2.4.1.2. Problemas con la Privacidad.

Las manifestaciones o confrontaciones sociales que estamos viviendo, el uso de la geolocalización es clave tanto para la organización entre las personas como para la localización de las mismas, convirtiéndose en un arma de doble filo para los usuarios.

En definitiva, el tema de la geolocalización y la privacidad es clave en estos tiempos, pero también depende del punto de vista que se adopte en torno al mismo:

- Desde el punto de vista de los usuarios, el control de la privacidad depende de la información que queramos dar y en este sentido podemos identificar dos aspectos:
  - El uso de la geolocalización en las redes sociales: cuando configuramos una cuenta, se nos suele preguntar sobre nuestro lugar de residencia y cuando interactuamos a través de las redes sociales la geolocalización aparece como opción, pero otras veces por defecto. En estos casos, si no queremos que se sepa dónde estamos o desde dónde generamos cierta información, podemos acudir a las mismas aplicaciones para desconectar la geolocalización y evitarlo.

- El uso de la geolocalización en general: hay que tener en cuenta que cualquier acción que desarrollemos en Internet con la geolocalización del teléfono o del ordenador activada deja siempre un rastro y, por tanto, es susceptible de ser localizado.

- Desde el punto de vista de los negocios, podemos utilizar estos datos siempre que sea de acuerdo con la ley y cumpliendo la protección de datos.

Asimismo, el Decreto Legislativo N° 1182 establece un procedimiento de investigación policial que vulnera derechos fundamentales y, en consecuencia, ***genera prueba prohibida que no podrá ser empleada en el proceso penal.*** (Elías. R, 2016. p. 8)

Además, la flagrancia delictiva exige inmediatez temporal y personal para su configuración. El uso de dispositivos móviles o electrónicos no permiten la configuración de ninguno de los cuatro supuestos previstos en el Código Procesal Penal para su aplicación. (Elías. R, 2016. p. 8). Por último, el Decreto Legislativo N° 1182 restringe las funciones del Ministerio Público y confunde los roles de la Fiscalía con los de la Policía al conferirle tácitamente a esta última la facultad de analizar jurídicamente y restringir derechos. (Elías. R, 2016. p. 8)

2.5. Hipótesis.

Con la implementación del Decreto Legislativo N° 1182, sobre geolocalización, en los delitos de crimen organizado sin autorización judicial por la DIVINCRI en el Distrito de Cajamarca:

- Se vulnera el derecho fundamental de la intimidad.
- Los procedimientos del decreto del decreto legislativo 1182 no se cumplen de manera adecuada, siendo estos ineficientes.
- La legislación comparada regula el acto de investigación de geolocalización en la norma penal y norma especial, respaldando la facultad del efectivo PNP de hacer uso de la geolocalización sin autorización judicial.

2.6. Operacionalización de Variables.

2.6.1. Variables.

En todo estudio de investigación en ciencias sociales, las variables se pueden definir como todo aquello que vamos a medir, controlar y estudiar en una investigación o estudio. Es importante, antes de iniciar una investigación, que se separe cuáles son las variables que se van a medir y la manera de cómo realizarlo.

2.6.1.1. Variable Independiente.

La variable independiente es todo aquello que el experimentador manipula, debido a que cree que existe una relación entre ésta y la variable dependiente. (Pick, S. y Velasco de la Fuente, A, 2002)

- Geolocalización.

2.6.1.2. Variable Dependiente.

La variable dependiente se define como los cambios sufridos por los sujetos como resultado de la manipulación de la variable independiente por parte del experimentador. (Pick, S. y Velasco de la Fuente, A, 2002)

- Derechos Fundamentales vulnerados.

2.6.1.3. Variable Interviniente.

La variable interviniente es aquella que estudian simultáneamente varios grupos de sujetos. (Pick, S. y Velasco de la Fuente, A, 2002)

- Derecho Comparado.

2.6.2. Operacionalización de variables.

VULNERACIÓN DEL DERECHO FUNDAMENTAL A LA INTIMIDAD CON LA IMPLEMENTACIÓN DEL DECRETO LEGISLATIVO N° 1182, SOBRE GEOLOCALIZACIÓN EN LOS DELITOS DE CRIMEN ORGANIZADO, SIN AUTORIZACIÓN JUDICIAL POR LA DIVINCRI EN EL DISTRITO DE CAJAMARCA – 2019				
Categorías	**Definición.**	**Dimensiones**	**Indicadores**	**Técnicas e Instrumentos**
Variable Independiente: Geolocalización	Capacidad para obtener la ubicación geográfica real de un objeto, como un radar, un teléfono móvil o un ordenador conectado a Internet.	mecanismos utilizados (dispositivos, equipos)	75 informes respecto de las denuncias de las víctimas por delitos de crimen organizado, registrado por el FRENPOL-CAJ-DIVINCRI-DEPINCRI-ARESE-SCG, durante el año 2019 en el Distrito de Cajamarca. Extorsión. Tráfico de Armas Trata de personas Pornografía infantil, entre otros	**Técnicas:** • Observación. • Línea de tiempo. • Fichas de resumen. • Fichas bibliográficas. • Registro de datos. **Instrumentos:** 75 informes emitidos por FRENPOL-CAJ-DIVINCRI-DEPINCRI-ARESE-SCG, durante el año 2019 en el distrito de Cajamarca. Analizar los presupuestos: •
Variable dependiente: Derechos Fundamentales	Son aquellos incluidos en la norma constitutiva y organizativa de un Estado generalmente denominada Constitución que se consideran como esenciales en el sistema político y que están especialmente vinculados a la dignidad humana.	Derechos vulnerados por aplicación de esta norma	Derecho a la intimidad.	
Variable Interviniente: Derecho Comparado	Disciplina que se basa en la comparación de ordenamientos jurídicos	Nacional e Internacionales	Análisis comparativo entre ordenamientos Jurídicos.	

CAPITULO III: METODOLOGÍA DE LA INVESTIGACIÓN.

3.1. Tipo de Investigación.

La presente investigación es de tipo Aplicada., De diseño descriptivo- explicativo, no experimental. De enfoque cualitativo y cuantitativo; pretende describir la realidad por la cual ha sido realizada la geolocalización sin autorización judicial, explicando las razones de dicha intervención; asimismo verificar los derechos fundamentales vulnerados.

Las investigaciones descriptivas miden o evalúan diversos aspectos o componentes del fenómeno a investigar. Trabaja sobre realidades de hechos y su característica fundamental es la de presentar una interpretación correcta.

Dentro de la investigación descriptiva, su preocupación primordial radica en descubrir características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios sistemáticos que permitan poner de manifiesto su estructura o comportamiento. De esta forma se pueden obtener las notas que caracterizan a la realidad estudiada. (González, Hernández y Viña, 2014)

Es explicativa, porque busca encontrar las razones o causas que provocan ciertos fenómenos; asimismo está dirigido a responder por las causas de los eventos y fenómenos físicos o sociales.

Se enfoca en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta, o por qué se relaciona dos o más variables. Su valor se encuentra más estructurado que las demás investigaciones, además de que proporcionan un sentido de entendimiento del fenómeno a que hace referencia. (Hernández, Fernández & Batista, 2010). En el nivel

cotidiano, sería investigar como el policía emplea la geolocalización, a una presunta comisión delictiva, establecida en el Decreto Legislativo N° 1182.

3.2. Diseño de Investigación.

El diseño de la presente investigación obedece a un modelo no experimental, descriptivo. Correlacional, transversal y analítico.

- ***No Experimental.*** El estudio del fenómeno es conforme se manifestó en su contexto natural; en consecuencia, los datos reflejan la evolución natural de los eventos, ajeno a la voluntad del investigador. (Hernández, Fernández & Batista, 2010)

- ***Retrospectiva.*** La planificación y recolección de datos comprende un fenómeno ocurrido en el pasado. (Hernández, Fernández & Batista, 2010)

- ***Transversal.*** La recolección de datos para determinar la variable, proviene de un fenómeno cuya versión corresponde a un momento específico del desarrollo del tiempo. (Hernández, Fernández & Batista, 2010)

- ***Correlacional.*** Porque tuvo como propósito ver la utilización de la geolocalización para localizar a presuntos autores de delitos, o que favorezcan a la investigación.

Esto, debe realizarse sin vulnerar los derechos fundamentales, tales como: derecho a la intimidad, derecho a la privacidad, derecho al secreto de las comunicaciones, y el derecho a la protección de datos, en el distrito de Cajamarca 2019. En síntesis:

Alcance	Propósito de las Investigaciones.	Valor
Descriptivo.	Busca especificar las propiedades, a las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro	Es útil para mostrar con precisión los ángulos o dimensiones de un fenómeno, suceso, comunidad, contexto o situación.

	fenómeno que se someta a un análisis.	
Correlacional.	Su finalidad es conocer la relación o grado de asociación que exista entre dos o más conceptos, categorías o variables en un contexto en particular.	En cierta medida tiene un valor explicativo, aunque parcial, ya que el hecho de saber que dos conceptos o variables se relaciona aporta cierta información explicativa.
Explicativo.	Está dirigido a responder por las cusas de los eventos y fenómenos físicos o sociales. Se enfoca en explicar por qué ocurre un fenómeno y en qué condiciones se manifiesta, o por qué se relacionan dos o más variables.	Se encuentra más estructurado que las demás investigaciones (de hecho, implica los propósitos de éstas); además de que proporciona un sentido de entendimiento del fenómeno a que hacen referencia.

Fuente: Metodología de la Investigación. (Hernández, Fernández & Batista, 2010)

3.3. Área de Investigación.

- Derecho Constitucional, al analizar los derechos fundamentales vulnerados, establecidos en el art. 2 de dicho cuerpo normativo.

- Derecho Penal, desde el punto de vista, de la delincuencia común y el crimen organizado a través del uso de tecnología de la información y comunicaciones por parte de la PNP.

3.4. Dimensión temporal y Espacial.

La dimensión temporal para esta investigación se encuentra determinada por el espacio de tiempo en que se desarrolló, al interesar comparar periodos, es de tipo longitudinal. Así, vamos a analizar los informes emitidos por el área encargada de comunicación y geolocalización del frente policial de la división de investigación de

criminalística del Distrito de Cajamarca. (FRENPOL-CAJ-DIVINCRI-DEPINCRI-ARESE-SCG), durante el año 2019.

3.5. Unidad de análisis, población y muestra.

- La unidad de análisis estuvo constituida por cada uno de los 73 informes emitidos por el FRENPOL-CAJ-DIVINCRI-DEPINCRI-ARESE-SCG. En el distrito de Cajamarca durante el año 2019.

- La Población constituida por el Distrito de Cajamarca, donde se obtuvo los 73 informes emitidos por el FRENPOL-CAJ-DIVINCRI-DEPINCRI-ARESE-SCG, donde se verificará los supuestos por el cual ha sido realizada la Geolocalización por parte de la PNP.

- La muestra constituida por 73 informes respecto de las denuncias de las víctimas por delitos de crimen organizado, registrado por el FRENPOL-CAJ-DIVINCRI-DEPINCRI-ARESE-SCG, durante el año 2019 en el Distrito de Cajamarca.

3.6. Métodos.

- **Sincrónico.** La sincronía es el tiempo en un momento dado, un tiempo concreto. En el presente proyecto será del análisis de informes emitidos por el FRENPOL-CAJ-DIVINCRI-DEPINCRI-ARESE-SCG, durante el año 2019 en el distrito de Cajamarca.

- **Exegético.** A través de la interpretación de normas. Plasmadas en el derecho positivo.

- **Dogmático Jurídico.** Contenido de las Normas Jurídicas Positivas, de la Justicia Comunal y de la Justicia Ordinaria, siguiendo de la lógica que otorga la dogmática jurídica.

- **Hermenéutico Jurídico.** Tiene como fin la interpretación de textos poco claros, en nuestro caso basado en la pluriculturalidad del país. Por lo que todo mensaje requiere ser interpretado, entre ellos los mandatos de las normas jurídicas, pero no es fácil lograr la correcta interpretación, si no se cuenta con reglas precisas y claras, metódicas y sistemáticamente establecidas.

  La hermenéutica jurídica es entendida, desde un punto de vista doctrinario como una disciplina científica que tiene por objeto el estudio y sistematización de los principios y métodos interpretativos.

  > Es en sí, la interpretación de la normativa Constitucional. La interpretación es aplicación de la hermenéutica. La hermenéutica es la teoría científica del arte de interpretar, descubriendo y determinando los principios que deben guiar la interpretación.

3.7. Técnica de Investigación.

Las técnicas de recolección de datos son las distintas formas o maneras de obtener la información deseada para la elaboración de una investigación. Estas dependen en gran parte del tipo de investigación y del problema planteado por la misma y pueden efectuarse desde la simple ficha bibliográfica, observación, entrevista, cuestionario o encuesta. (González, Hernández y Viña, 2014)

Una de las herramientas empleadas para el desarrollo del presente estudio fue el arqueo bibliográfico y cuestionario, que no es más que el uso sistemático de los sentidos de búsqueda de los datos que se necesitan para resolver un problema de investigación. La presente investigación se caracteriza por ser documental.

El investigador con el apoyo de un asesor, preparado y capacitado, observará de forma indirecta las variables a través de los indicadores de cada una de sus dimensiones. Las técnicas a desarrollar fueron las siguientes:

- *Primera etapa.* De manera abierta y exploratoria, que consistió en una aproximación gradual y reflexiva al fenómeno, orientada por los objetivos de la investigación en base a la recopilación de información teórica.

  - *Bitácora o diario de campo:* Es un documento que sirve para registrar ideas, observaciones y hacer bosquejos del trabajo de investigación, de tal forma que permita sistematizar ideas.

- *Segunda etapa.* En base a una actividad más sistémica, en términos de recolección de información (datos) para determinar los derechos vulnerados y los presupuesto por la cual se empleó la geolocalización establecido en el artículo 3 del Decreto Legislativo N° 1182, que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.

  - Recopilación documental: Permitirá recoger información

- *La tercera etapa.* Igual que las anteriores, más consistente, y que consistió de manera analítica y más profundo, donde habrá articulación entre los datos y la revisión de la literatura.

3.8. Procesamiento de análisis de datos.

La unidad de análisis corresponde a la entidad mayor o representativa de lo que va ser objeto específico de estudio en una medición y se refiere al que o quien es objeto de interés en una investigación en pocas palabras sin los elementos sobre los que se focaliza el estudio. (González, Hernández y Viña, 2014)

Procesar información significa analizarla, delimitar en ella los hechos, conceptos,

distinguir las posiciones principales del autor, las argumentaciones, sistematizar o reorganizar lógicamente el contenido, resumirlo". (González, Hernández y Viña, 2014).

El procesamiento de la información es un continuo que va desde un procesamiento superficial, pasando por uno intermedio hasta llegar al más profundo, de carácter semántico, de construcción de significado. La persistencia de la información que almacenamos en nuestra memoria está en función de la profundidad del análisis.

En consecuencia, los niveles de análisis más profundos permiten que dicha información sea más elaborada, más fuerte y más perdurable. A mayor grado de análisis semántico, mayor profundidad de procesamiento" (Gómez. J, 2004; p.289).

El procesamiento de la información a partir del documento científico es concebido como una red de ideas interconectadas y como una trama de intenciones elaborada o reconstruida por los comunicantes en función de los esquemas de conocimientos compartidos. (Lancaster. F y Pinto. M, 2001 p.2010).

El análisis de la información significa descompones un todo en su parte constitutiva para un examen minucioso. Es la etapa en la que tienes que realizar inferencias válidas y confiables en el contexto que se han obtenido. Esta se realizará en base a criterios de:

- Integración lógica para la presentación del discurso.
- Comentario crítico de los resultados en su significación actual y en función a los objetivos de investigación previstos.
- Coordinación de los resultados obtenidos en torno al nivel de uso de la interpretación con las teorías.

En el presente proyecto de investigación el análisis será de manera cualitativo puesto

que es un proceso de categorización e interpretación para dar explicación al fenómeno objeto de la investigación.

3.9. Instrumentos.

De los instrumentos durante esta actividad se evidenció desde el instante, que el investigador aplicó la observación y el análisis en el objeto de estudio; los informes emitidos por el área de investigación de criminalística DIVINCRI. Acto seguido, el investigador con ayuda de mayor dominio de las bases teóricas, manejó la técnica de la observación y el análisis de contenido; orientado por los objetivos específicos se llevó el recojo de datos.

3.10. Limitaciones de la Investigación.

La presente tesis, durante su desarrollo, tuvo como principal limitación la falta de tiempo para poder realizar un estudio más exhaustivo del área de la DIVINCRI, a fin de poder recopilar más información.

3.11. Aspectos Éticos de la Investigación.

Esta Investigación se fundamentó en criterios dirigidos a asegurar la calidad y la objetividad de la investigación como los siguientes:

- **Autonomía:** Dicha investigación fue realizada por nuestra autonomía al realizar el recojo personalmente acudiendo en varias oportunidades al área de la división de investigación de criminalista (DIVINCRI). También, los aspectos éticos se verán plasmados en el no plagio de otras investigaciones, asegurando la autoría de lo escrito, habiéndose citado toda la información que se haya tomado de otro autor.

- **No maleficencia.** La información se obtuvo luego que el Brigadier Calderón Movallón, quien es el encargado de dicha área, diera consentimiento y autorización para acceder a la información que fue materia de estudio.

- **Privacidad:** Se respeta el anonimato de las personas que intervienen en dichos informes.

CAPITULO IV: RESULTADOS Y DISCUSIÓN.

4.1. Resultados.

Tabla N° 1. Para que se empleó El uso de las TICs (*) y TIGs (**).

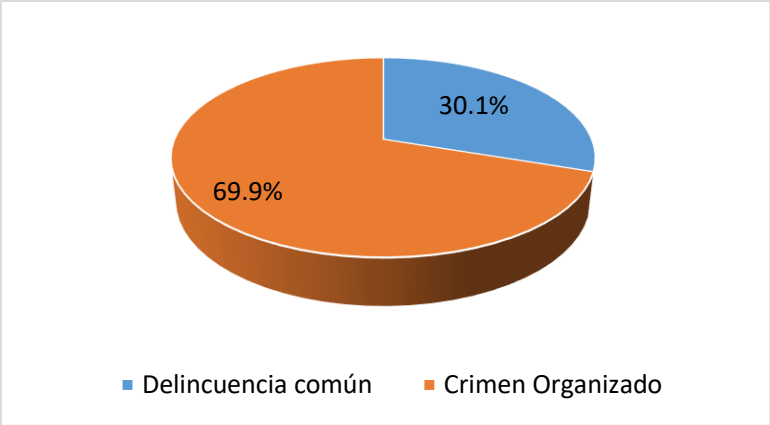
El uso de las TICs y TIGs se empleó en la investigación .	N°	%
Delincuencia común	22	30.1
Crimen Organizado	51	69.9
Total	**73**	**100.0**

Fuente: Elaboración Propia.

(*) Tecnología de la Información y Comunicaciones.

(**) Tecnología de la información Geográfica.

Gráfico N° 1. El uso de las TICs (*) y TIGs (**) se empleó para investigar.



Fuente: Elaboración Propia.

Interpretación. En la presente tabla se muestra que el 30.1% equivalente a 22 informes han sido empleado para la investigación de delincuencia Común. En los que se encuentra extorsión, secuestro, asaltos, robos a mano armada. Asesinato (sicariato), estafa, piratería informática. los casos de delitos cometidos desde el interior de los establecimientos penales a nivel nacional, principalmente por los delitos de homicidio calificado (en la modalidad de sicariato), secuestro, trata de personas, extorsión, contra el patrimonio, tráfico ilícito de drogas, entre otros.

Conforme a datos obtenidos de la Policía Nacional del Perú ante esta situación, a través del Sistema de Geolocalización de la DIVINDAT/DIRINCRI PNP, establecieron estadísticamente que la más alta incidencia de llamadas extorsivas, se han presentado provenientes de los establecimientos penitenciarios

Un 69.9% equivalente a 51 informes han sido empleadas para investigar casos relacionados con el crimen organizado, en los que encontramos: trata de personas, tráfico de drogas, mercancías ilícitas y armas, robo a mano armada, falsificaciones y blanqueo de capitales.

Caso Analizado: INFORME Nº 511-2019 -SCG-FRENPOL-CAJ/DIVINCRI-DEPINCRI-ARESE.

Delito: por la presunta comisión del Delito Contra el Patrimonio – Extorsión, hecho ocurrido el día 05NOV2019, en horas de tarde, en esta ciudad de Cajamarca.

Competencia : Tercera Fiscalía Provincial Penal Corporativa Cajamarca.
Abogado. Jesús PORTAL CASTREJON – Fiscal.

Referencia : - Acta de Denuncia N° 418 – 2019., del 05NOV2019

Datos: En el Barrio Chonta Paccha - Cajamarca, celular N° 961 XXX XXX quien con conocimiento del Jefe DEPINCRI y del R.M.P J. P. C. - Fiscal de la 3° Fiscalía Provincial Penal Corporativa - Cajamarca; denuncia que está siendo víctima de la presunta comisión del delito de extorsión, toda vez que el 05NOV2019, a horas 12:30 aprox. ha recibido llamadas telefónicas, mensajes de texto y WhatsApp del celular N° 995 XXX XXX, asimismo el denunciante refiere que desconoce quién es el propietario del celular N° 995 XX XXX, el denunciante hace mención que, le han solicitado la suma de quince mil soles (S/.15 000.00), para que no atenten contra su vida, también le han enviado fotos a su WhatsApp personal, las fotos son del denunciante, de una de sus trabajadoras, y le hacen mención del nombre de uno de sus compañeros de trabajo, a la vez le indican que no vaya ante la policía porque si no le van a matar; ante tal hecho el denunciante hace de conocimiento a la PNP para los fines correspondientes. Siendo las 18:20 horas del mismo día se da por concluida la presente diligencia, firmando a continuación el denunciante en señal de conformidad, en presencia del instructor que certifica

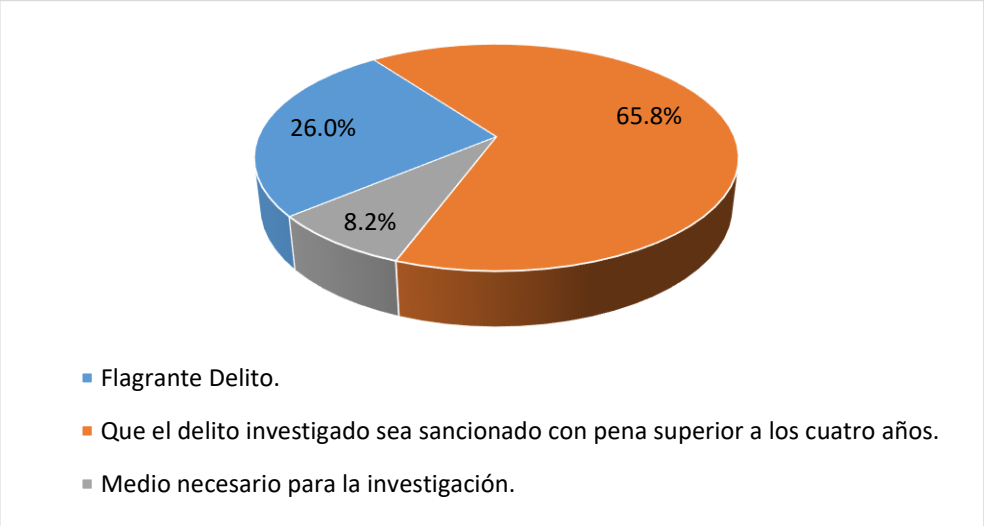
Es decir, un hombre denunció en la 1era. Comisaria de Cajamarca, que viene siendo extorsionado. Dijo que los supuestos delincuentes lo llamaban desde un celular y le pedían S/. 15.000.00 mil soles, para no matarlo a él o su familia. El número de ese teléfono fue clave para conocer la verdad. El caso fue derivado al nuevo Departamento de Geolocalización de la Policía, situado en la Dirección de investigación Criminal (Dirincri) del Jr. Amalia Puga. Los agentes solicitaron la ubicación de este celular a la empresa operadora. En solo una hora ya se sabía que el secuestrador se comunicaba desde el Penal de Huacariz. De inmediato, la Policía fue al lugar y encontró al sujeto de iniciales A.R.CH.

Tabla N° 2. Procedencia del presupuesto por el cual se empleó la Geolocalización.

Presupuesto	N°	%
Flagrante Delito.	19	26.0
Que el delito investigado sea sancionado con pena superior a los cuatro años.	48	65.8
Medio necesario para la investigación.	6	8.2
Total	**73**	**100.0**

Fuente: Elaboración Propia.

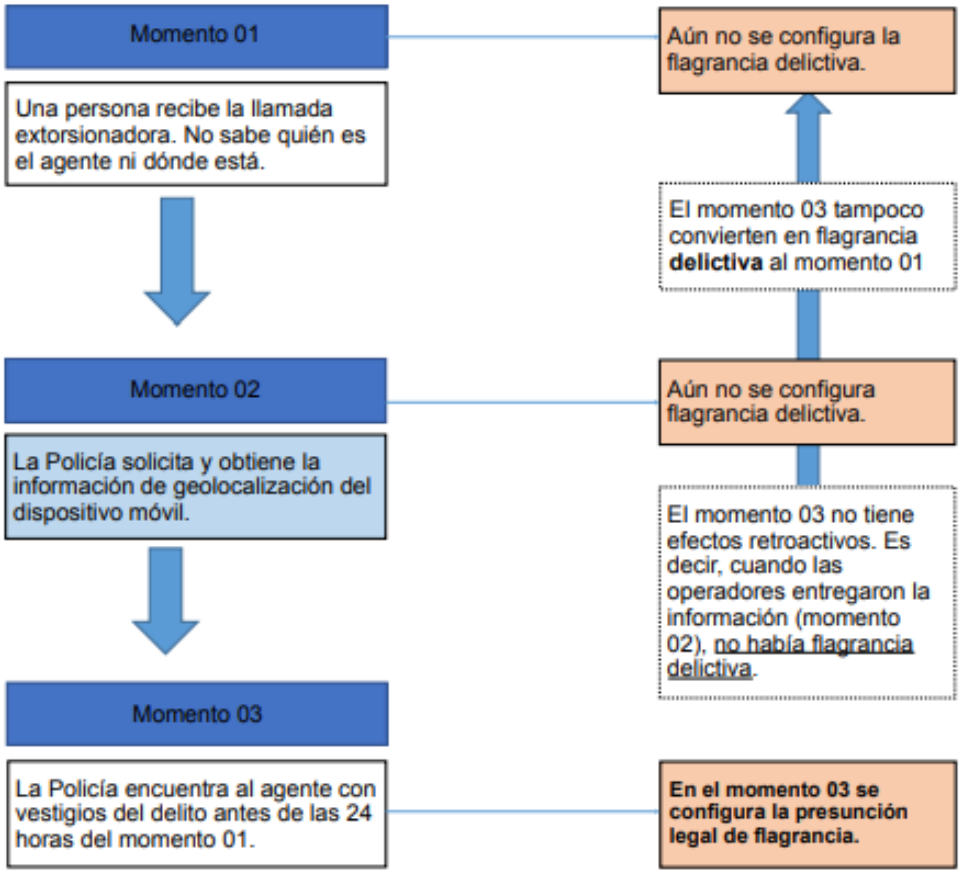
Gráfico N° 2. Procedencia del presupuesto por el cual se empleó la Geolocalización.



Fuente: Elaboración Propia.

Interpretación. En la presente tabla se ha encontrado que 26% equivalente a 19 informes están relacionadas a flagrancias delictivas. Un 65.8% equivalente a 48 informes a delitos donde la pena sea sanciona con una pena privativa de libertad de cuatro años.

Por último, tenemos que el 8.2% equivalente a 6 informes relacionado a medios que son necesarios para la investigación.



Caso Analizado: INFORME Nº 327-2019-SCG-FRENPOL-CAJ/DIVINCRI-DEPINCRI-ARESE.

Delito: por la presunta comisión Delitos contra el cuerpo la vida y la salud – Trata de personas, hecho ocurrido el día 24 JUN2019, en horas de tarde, en esta ciudad de Cajamarca.

Competencia : Tercera Fiscalía Provincial Penal Corporativa Cajamarca.
Abogado. J. P. C.– Fiscal.

Referencia : - Acta de Denuncia N° 787 – 2019., del 24JUN2019

Datos: En el Barrio El estanco - Cajamarca, celular N° 961 XXX XXX quien con conocimiento del Jefe DEPINCRI y del R.M.P J. P. C. - Fiscal de la 3° Fiscalía Provincial Penal Corporativa - Cajamarca; denuncia que está siendo víctima de la presunta comisión del

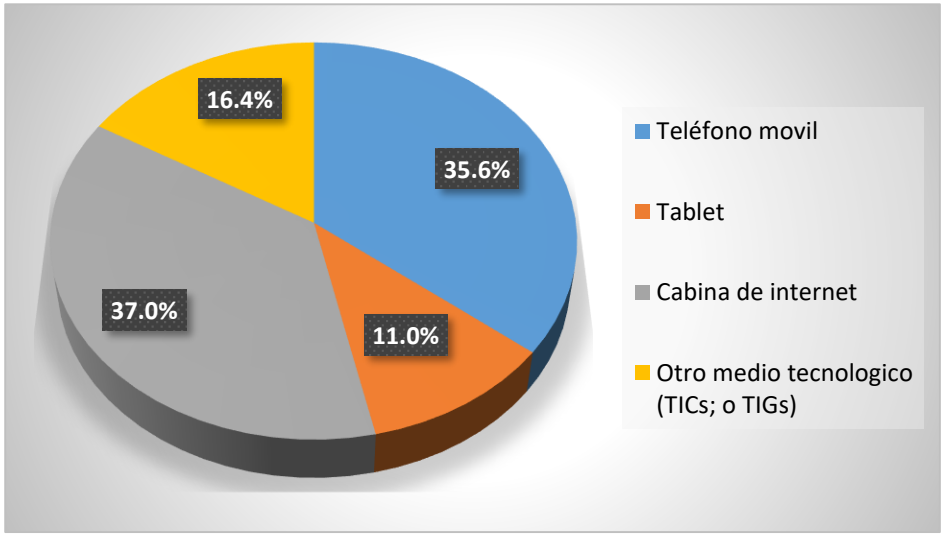
delito contra el cuerpo la vida y la salud – Trata de personas, rapto de menor de edad, a horas 10:30 aprox. Del día 22JUN19 ha recibido llamadas telefónicas, mensajes de texto y WhatsApp del celular N° 976 XXX XXX, asimismo el denunciante refiere que desconoce quién es el propietario del celular N° 976 XX XXX, el denunciante hace mención que, le han indicado que el menor ha sido trasladado al país de Colombia y que no haga denuncia alguna o devolverán el cuerpo en pedazos , también le han enviado fotos a su WhatsApp personal, , a la vez le indican que no vaya ante la policía porque si no le van a matar; ante tal hecho el denunciante hace de conocimiento a la PNP para los fines correspondientes. Siendo las 12:20 horas del mismo día se da por concluida la presente diligencia, firmando a continuación el denunciante en señal de conformidad, en presencia del instructor que certifica

Tabla N° 3. Dispositivo de Ubicación

Dispositivo de ubicación	N°	%
Teléfono móvil	26	35.6
Tablet	8	11.0
Cabina de internet	27	37.0
Otro medio tecnológico (TICs; o TIGs)	12	16.4
Total	**73**	**100.0**

Fuente: Elaboración Propia.

Gráfico N° 3. Dispositivo de Ubicación



Fuente: Elaboración Propia.

Interpretación. En la presente tabla se muestra un 35.6% equivalente a 26 informes que la geolocalización fue efectuada a un teléfono móvil, (movistar, entel, bitel, claro). Un 11.0% equivalente a 8 informes se ubicación la geolocalización por la señal Wii Fi. Que utilizo para acceder a información. Un 37.0 % equivalente a 27 informes se relaciona con cabinas de internet a través de las direcciones IP. Por último, un 16.4% equivalente a 12 informes por otro tipo de dispositivo. GPS.

La División de Investigación de Secuestros DIRINCRI PNP, con fecha 26FEB2019, ejecutó la Orden de Operaciones Antisecuestros y Extorsiones "Norteño-2019" DIRINCRI/DIVINSE, en el establecimiento penitenciario de "PICSI", con el objetivo de registrar los pabellones

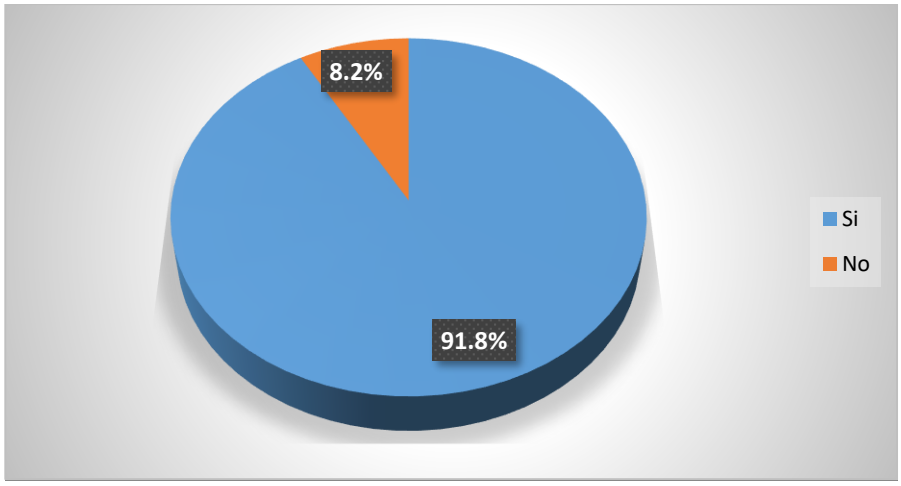
C y de Máxima Seguridad en Régimen Cerrado Especial, donde se encuentran recluidos los integrantes de las organizaciones criminales "Barrio King"; "Los Intocables de Chimbote"; "Dragones Rojos Nueva Generación"; "Los Charlys de Chiclayo"; "Los Piratas"; "Los Sicarios del Norte"; y, "Los Malditos de Cono Sur"; todo ello, al tenerse conocimiento que dichas organizaciones criminales estarían efectuando llamadas telefónicas extorsivas a potenciales víctimas a nivel nacional y como consecuencia de la operación policial antes referida.

Tabla N° 4. La unidad a cargo de la investigación policial una vez verificado puso de conocimiento al Ministerio Público el hecho y formula el requerimiento a la unidad especializada de la PNP para efectos de la geolocalización.

La unidad a cargo de la investigación policial una vez verificado puso de conocimiento al Ministerio Público el hecho y formula el requerimiento a la unidad especializada de la policía nacional del Perú para efectos de la localización o geolocalización.	N°	%
Si	67	91.8
No	6	8.2
Total	**73**	**100.0**

Fuente: Elaboración Propia.

Gráfico N° 4. La unidad a cargo de la investigación policial una vez verificado puso de conocimiento al Ministerio Público el hecho y formula el requerimiento a la unidad especializada de la policía nacional del Perú para efectos de la localización o geolocalización.



Fuente: Elaboración Propia.

Interpretación. En la presente tabla se muestra que un 91-8% equivalente a 67 informes emitidos, la unidad de investigación puso conocimiento a representante del Ministerio Público para hacer el empleo de la investigación, en casos de delincuencia común o crimen organizado, en relación a los presupuestos establecidos en el art. 3 del D. L. n° 1182, tales presupuestos son: cuando se trate de flagrante delito, de conformidad con lo dispuesto en el artículo 259 del decreto legislativo nº 957, código procesal penal; b. cuando el delito

investigado sea sancionado con pena superior a los cuatro años de privación de libertad. Y que el acceso a los datos constituya un medio necesario para la investigación. Asimismo, se muestra un 8.2% equivalente a 6 informes no realizó el comunicado al representante del Ministerio Público, en el plazo establecido por causas ajenas a su responsabilidad.

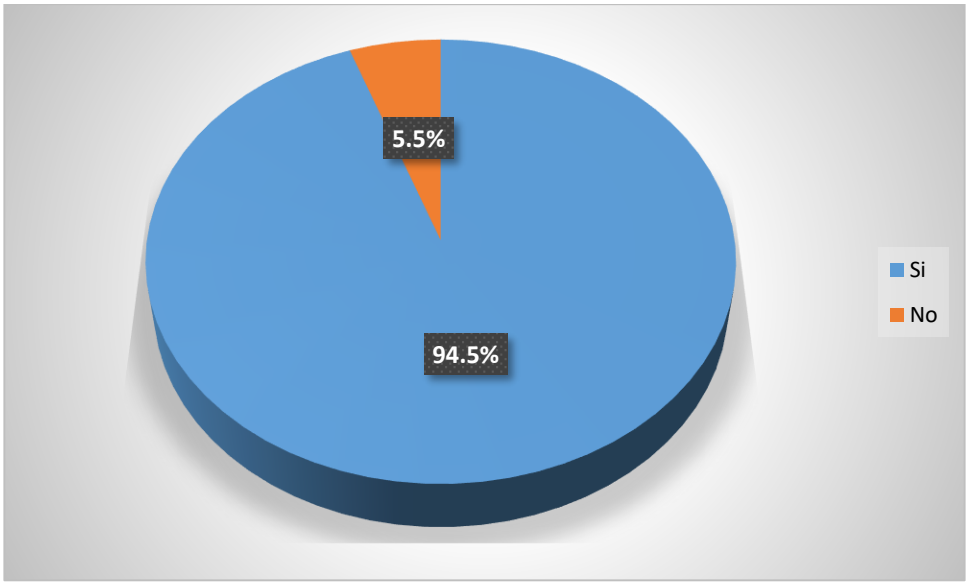
Tan pronto la Policía tenga noticia de la comisión de un delito, pondrá de conocimiento al Ministerio Público por la vía más rápida y también por escrito, indicando los elementos esenciales del hecho y demás elementos inicialmente recogidos, así como la actividad cumplida, sin perjuicio de dar cuenta de toda la documentación que pudiera existir.

Tabla N° 5. La unidad de la PNP cursa el pedido a los concesionarios de telecomunicaciones para acceder a los datos de geolocalización.

La unidad de la PNP cursa el pedido a los concesionarios de telecomunicaciones para acceder a los datos de geolocalización.	N°	%
Si	69	94.5
No	4	5.5
Total	**73**	**100.0**

Fuente: Elaboración Propia.

Gráfico. N° 5 La unidad de la PNP cursa el pedido a los concesionarios de telecomunicaciones para acceder a los datos de geolocalización.



Fuente: Elaboración Propia.

Interpretación. En la presente tabla se muestra que un 94.5% equivalente a 69 informes en representante de la unidad de investigación de la PNP, solicitó a empresa concesionaria del servicio, acceder al servicio de geolocalización. Un 5.5 % equivalente a 4 informes no realizó dicha solicitud, realizando la geolocalización por iniciativa, ocasionando perjuicio al presunto investigado. (el presunto autor o tercero vinculado al autor por rasgo de parentesco, sin tener nada que ver en la investigación).

Los concesionarios o servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, están obligados a brindar los datos de localización o geolocalización de manera inmediata, las veinticuatro (24) horas del día de los trescientos sesenta y cinco (365) días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento (artículo 4.3). Sé que el término "inmediato" aumenta los riesgos al condicionar la aplicación de esta facultad excepcional a casos de flagrancia.

Ejemplo.: El 1 de enero de 2016 a las 00:00 recibimos una llamada extorsionadora. Acudimos a la Policía a las 18:00, mientras se realizan las comunicaciones respectivas pasan algunas horas y la Unidad Especializada remite la comunicación a la operadora a las 23:00 y esta responde a las 01:00. A quienes aún consideren que sólo se requiere inmediatez temporal y no personal para la configuración de la flagrancia, la pregunta es ¿qué harían con la información recibida pues aun cuando encontrasen al agente? Al haber pasado más de 24 horas, este no podrías detenido. Es más, habrían recibido la información cuando la flagrancia (que se considera no se configura) ya habría cesado. (Elías. R, 2016)

la ley procesal establece dentro de los alcances de la medida de levantamiento de 34 secreto de comunicaciones dictada por el juez, la obligación de las empresas concesionarias de brindar la geolocalización de teléfonos móviles, e inclusive dicha norma es más clara porque establece que dicha medida podrá dictarse no sólo contra el investigado sino también contra personas de las que cabe estimar fundadamente, en mérito a datos objetivos determinados que reciben o tramitan por cuenta del investigado determinadas comunicaciones, o que el investigado utiliza su comunicación. De esta forma, quedan en evidencia las ambigüedades, vacíos y contradicciones que trae consigo el Decreto Legislativo N° 1182, cuyo problema central radica en haberse otorgado facultades a la Policía para

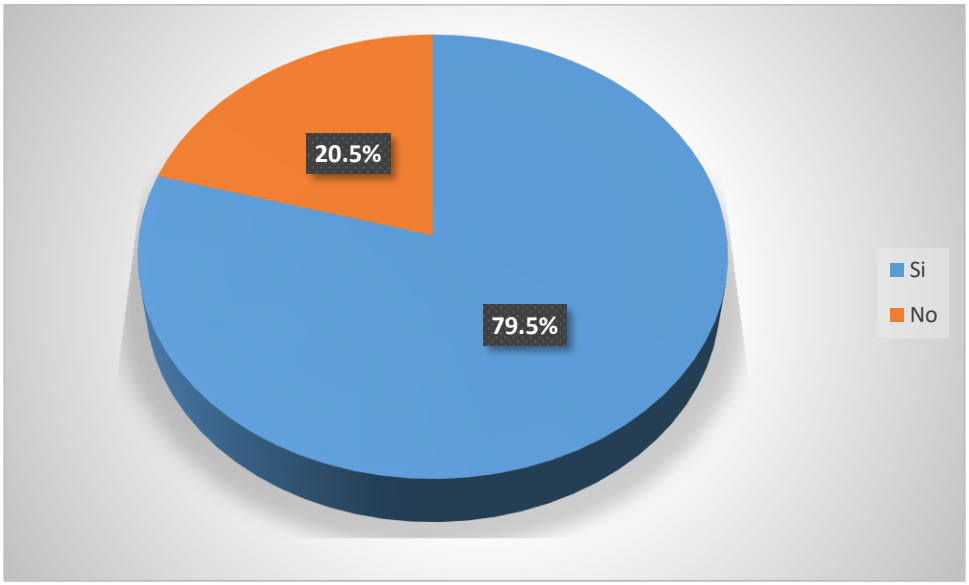
solicitar la intervención de comunicaciones para la identificación, localización y geolocalización de equipos, sin orden ni control judicial alguno. (Caro C., 2015)

Tabla N° 6. La unidad a cargo de la investigación policial realiza las diligencias pertinentes.

La unidad a cargo de la investigación policial realiza las diligencias pertinentes.	N°	%
Si	58	79.5
No	15	20.5
Total	**73**	**100.0**

Fuente: Elaboración Propia.

Gráfico N° 6. La unidad a cargo de la investigación policial realiza las diligencias. pertinentes



Fuente: Elaboración Propia.

Interpretación. En la presente tabla se muestra que un 79.5% equivalente a 58 informes, Asimismo, Un 20.5 % equivalente a 15 informes **se** mostró que la unidad de investigación no realizo el requerimiento al ministerio Público en el plazo establecido.

Los artículos 4 y 5 del Decreto Legislativo regulan el procedimiento policial para acceder a la ubicación de los dispositivos electrónicos y el pedido de convalidación judicial. Los pasos

que sigue este procedimiento especial y demostraremos que existen vicios: el sacrificio de garantías en aras de una supuesta eficacia investigativa.

La unidad a cargo de la investigación policial, una vez verificados los supuestos del artículo, pone en conocimiento del Ministerio Público el hecho y formula el requerimiento a la unidad especializada de la Policía Nacional del Perú para efectos de la localización o geolocalización (artículo 4.1). La norma condiciona la puesta en conocimiento de los hechos denunciados a una previa verificación a cargo de la Policía de los supuestos, que, impide tratar los delitos cometidos a través de dispositivos móviles bajo la figura de flagrancia delictiva. Dicho de otro modo, la redacción es tendenciosa pues, de acuerdo al artículo 331.1 del Código Procesal Penal, la Policía debe de comunicar inmediatamente la denuncia formulada por un ciudadano ante su dependencia y no condicionarlo a la verificación previa de los referidos supuestos. (Elías. R, 2016)

La unidad especializada de la Policía Nacional del Perú que recibe el requerimiento, previa verificación del responsable de la unidad solicitante, cursa el pedido a los concesionarios de los servicios públicos de telecomunicaciones o a entidades públicas relacionadas con este servicio, a través del correo electrónico institucional u otro medio idóneo convenido (artículo 4.2). Los argumentos por los que la Policía no tiene la facultad constitucional de solicitar datos de localización o geolocalización a las empresas de comunicación al encontrarse protegidas por el derecho fundamental del secreto de las comunicaciones. No se ha tenido acceso al protocolo que regula el procedimiento que estamos analizando; sin embargo, la Policía ya hace uso de esta facultad. Se espera que todo el circuito de comunicación -desde el registro de la denuncia, la comunicación al Ministerio Público, así como a la Unidad Especializada, la verificación del responsable hasta los correos electrónicos de solicitud y de respuesta de las operadoras- se encuentre anexo a la carpeta fiscal pues, de lo

contrario, se estaría restringiendo el derecho a la defensa ya que no tendría la posibilidad de verificar cómo se desarrolló el procedimiento. (Elías. R, 2016)

La unidad a cargo de la investigación policial realiza las diligencias pertinentes en consideración de la información obtenida y a otras técnicas de investigación, sin perjuicio de lo establecido en el artículo 5 (artículo 4.4). Que la Policía realice actos de investigación no genera problema alguno, pues forman parte de sus funciones conforme se encuentra previsto en el artículo 67 del Código Procesal Penal., salvo detención policial o allanamiento en flagrancia, no está facultada constitucionalmente a restringir nuestro derecho al secreto de las comunicaciones. (Elías. R, 2016)

La unidad policial a cargo de la investigación policial, dentro de las 24 horas de comunicado el hecho al Fiscal correspondiente, le remitirá un informe que sustente el requerimiento para su convalidación judicial (artículo 5.1). El Fiscal dentro de las veinticuatro (24) horas de recibido el informe, solicita al Juez la convalidación de la medida (artículo 5.2). La redacción es inadecuada y sugiere que en todos los casos el Fiscal solicitará la convalidación judicial. Nuevamente, el titular de la acción penal es el Fiscal y, de acuerdo al artículo 60.2 del Código Procesal Penal: “El Fiscal conduce desde su inicio la investigación del delito. Con tal propósito la Policía Nacional está obligada a cumplir los mandatos del Ministerio Público en el ámbito de su función.”

En consecuencia, pese a que la norma no lo expresa, si el Fiscal no está de acuerdo con la solicitud de la Policía tiene toda la potestad de ordenar se deje sin efecto la medida. El problema surgirá cuando la Policía haya obtenido información relacionada a la localización o geolocalización y después la Fiscalía muestre su disconformidad con tal pedido: ¿qué sucede con la información?, ¿quién se responsabilizará por la lesión sufrida por el ciudadano afectado? Al no contar con el Protocolo de actuación (porque el Ejecutivo le ha conferido la

condición de información reservada) no sabemos de qué forma la Fiscalía comunicaría la revocatoria de la solicitud policial a la operadora de telefonía: ¿directamente?, ¿a través de la Unidad Especializada de la Policía?, ¿a través de la Unidad de Investigación? (Elías. R, 2016)

El juez competente resolverá mediante trámite reservado y de manera inmediata, teniendo a la vista los recaudos del requerimiento fiscal, en un plazo no mayor de 24 horas. La denegación del requerimiento deja sin efecto la medida y podrá ser apelada por el Fiscal. El recurso ante el juez superior se resolverá en el mismo plazo y sin trámite alguno (artículo 5.3). El juez que convalida la medida establecerá un plazo máximo que no excederá de sesenta (60) días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del Fiscal (artículo 5.4).

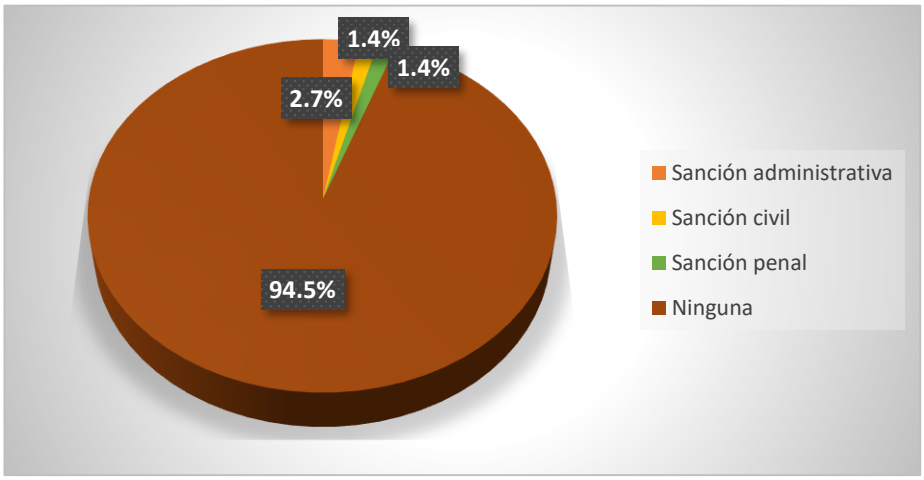
Este último paso debió ser el segundo en el procedimiento –el primero, obviamente, sería la comunicación y solicitud a cargo del Fiscal–. Ya que toda norma es perfectible, consideramos que, en una eventual reforma, debería establecerse, al igual que en artículo 230 del Código Procesal Penal, que la resolución judicial debería indicar la información a la cual la Fiscalía puede acceder. Esto impedirá que la convalidación judicial sea tomada como un "cheque en blanco" que autoriza cualquier solicitud de información relacionada a la localización. Sin esta precisión, la Fiscalía o la Policía podrían solicitar ubicaciones históricas que no se encuentran vinculadas a la investigación criminal y, de este modo, lesionar el derecho a la intimidad personal. (Elías. R, 2016)

Tabla N° 7. Responsabilidad por uso indebido de geolocalización.

Responsabilidad por uso indebido de geolocalización.	N°	%
Sanción administrativa	2	2.7
Sanción civil	1	1.4
Sanción penal	1	1.4
Ninguna	69	94.5
Total	**73**	**100.0**

Fuente: Elaboración Propia.

Gráfico N° 8. Responsabilidad por uso indebido de geolocalización.



Fuente: Elaboración Propia.

Interpretación. En la presente tabla, se muestra que un 2.7% equivalente a 2 informes el encargado de realizar los procedimientos establecidos en el D. L. 1182, ha cometido errores en la tramitación de la documentación, acarreando sanción administrativa.

UN. 1.4% equivalente a 1 informe, tendrá sanción civil, en lo que respecta a uns reparación civil por daños y perjuicios ocasionado.

Un 1.4 equivalente a 1 informe, conllevo a una sanción penal por motivos que al emplear la geolocalización fue para usos personales.

UN 94.5% equivalente a 69 informes no acarreo ningún tipo de sanción.

Asimismo, se establece las responsabilidades sean de tipo administrativo, civil y penal para los concesionarios de servicios públicos de telecomunicaciones, que incumplan o demoren en atender la solicitud requerida por la Unidad Especializada, con lo cual se busca lograr que las unidades policiales de investigación, cuenten con la información de manera oportuna y resolver el hecho de contenido criminal con la eficacia que la ciudadanía espera de los operadores de seguridad y justicia.

4.2. Discusión.

4.2.1. Variable Geolocalización.

Se implementan con el fin de obtener información en tiempo real que facilite principalmente la investigación de los delitos, pero también se pueden emplear para la ubicación de personas desaparecidas, el seguimiento de actividades posiblemente delictivas, la represión de activistas y líderes de movimientos sociales, entre otros.

El Decreto Legislativo afecta derechos fundamentales El artículo 6 del Decreto Legislativo precisa que se "***excluyen expresamente cualquier tipo de intervención de las telecomunicaciones, las que se rigen por los procedimientos correspondientes."*** Es decir, el Ejecutivo trata de evitar cuestionamientos relacionados a la restricción de derechos fundamentales en la búsqueda y obtención de medios de pruebas. Sin embargo, se considera que sí se afectan tanto el derecho al secreto de las comunicaciones (artículo 2.10 Const.), a la intimidad (artículo 2.7 Const.) como a la autodeterminación informativa (artículo 2.6 Const.). (Elías. R, 2016. p. 8)

Pese a que esto, sí es necesario advertir que el Estado, al ordenar que se efectúe una audiencia de convalidación de la facultad policial, reconoce que se están afectando derechos fundamentales pues, de lo contrario, esta diligencia sería innecesaria.

No se debe olvidar que con las nuevas tecnologías lo que se transmite no sólo es el contenido (mensaje) sino también información relacionada al emisor, sea de manera consciente o inconsciente. Así, al inicio, cada llamada o mensaje que enviamos a través de las redes móviles o las nuevas tecnologías está compuesta por datos de información de la transmisión y de contenido. Si se justifica realizar un trato

diferenciado entre ambas pues la exigencia será mucho mayor en el caso de una intervención telefónica y menor cuando se requiera la ubicación del dispositivo. Esto no justifica excluir de su protección a una de ellas.

Al tratar de demostrar que es imposible jurídicamente que se encuentre ante supuestos de flagrancia que habiliten la geolocalización del presunto agente, ya que dicha figura requiere dos elementos***: inmediatez temporal e inmediatez personal. Este último no se encuentra presente en los delitos cometidos a través de dispositivos móviles o similares. Prescindir de la inmediatez personal ampliaría peligrosamente la figura de flagrancia delictiva.*** (Elías. R, 2016. p. 8)

Por otro lado, ***el Decreto Legislativo no restringe la geolocalización a casos de extorsión, trata de personas u otros delitos muy graves*** como fue planteada inicialmente, sino virtualmente a todo tipo de delitos previstos en el Código Penal. Además, ***el Decreto Legislativo exige que sea el Policía y no el Fiscal quien evalúe la necesidad, sub-principio que integra el principio de proporcionalidad, de restringir un derecho fundamental; es decir, propicia la confusión jurídica de roles.*** (Elías. R, 2016. p. 8)

En primer lugar, la única posibilidad de aplicar el Decreto Legislativo es eliminando (peligrosamente) la inmediatez personal como requisito de la flagrancia delictiva. En efecto, respecto al primer requisito, el Tribunal Constitucional ha establecido que de manera copulativa y no disyuntiva debe de reunirse criterios de inmediatez temporal y personal para su aplicación.

De esta forma, el Supremo Intérprete en los pronunciamientos más recientes ha establecido: 26 (…) que la flagrancia en la comisión de un delito presenta la concurrencia de dos requisitos insustituibles: ***a) la inmediatez temporal, es decir, que***

el delito se esté cometiendo o que se haya cometido antes; y b) la inmediatez personal, es decir, que el presunto delincuente se encuentre en el lugar de los hechos en el momento de la comisión del delito y esté relacionado con el objeto o los instrumentos del delito, ofreciendo una prueba evidente de su participación en el hecho delictivo."

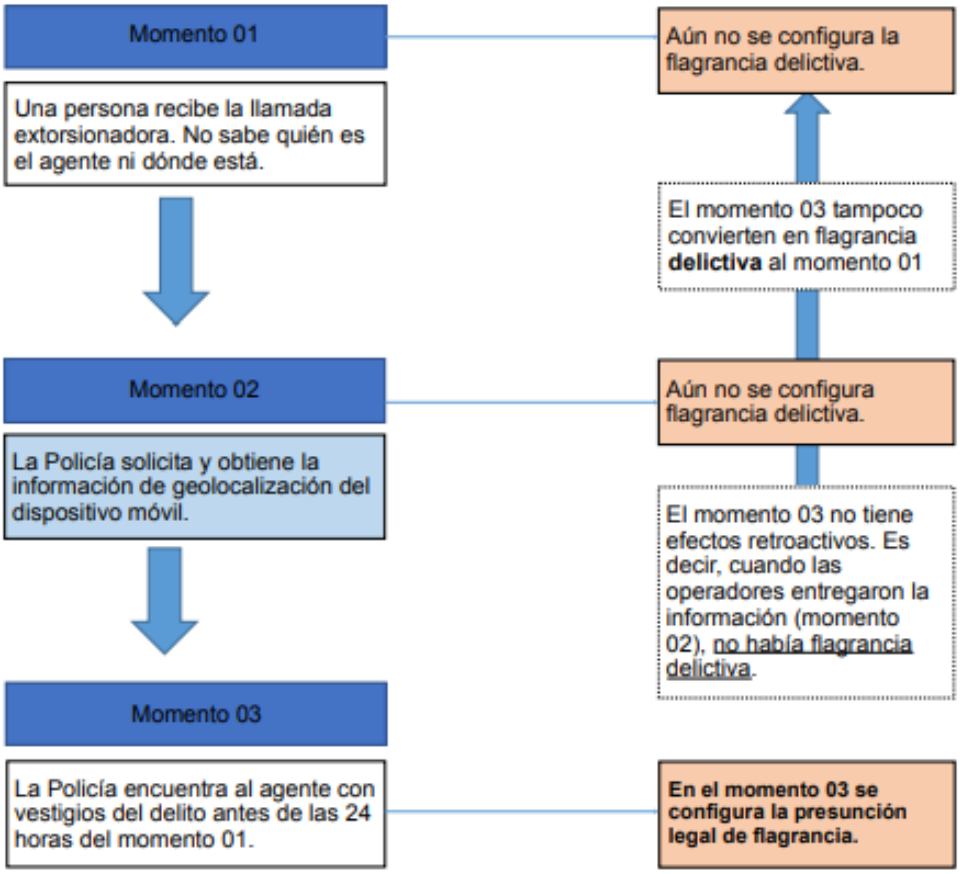
Al analizar los cuatro supuestos de flagrancia previstos en el artículo 259 del Código Procesal Penal caemos en cuenta que estos no cobijan aquellos casos para los que el Decreto Legislativo fue promulgado.

Ejemplo: acabamos de recibir una llamada exigiéndonos un monto de dinero para que nuestro negocio no sea incendiado. La pregunta es: ¿en cuál de los cuatro supuestos de flagrancia nos encontramos: ¿flagrancia clásica, cuasifagrancia, flagrancia por indicios o presunción de flagrancia?

- No nos encontramos frente a la flagrancia clásica o flagrancia propiamente dicha pues el agente no ha sido descubierto mientras está realizando el hecho punible. Es más, no sabemos quién es este mientras se lleva a cabo la llamada.
- El agente tampoco ha sido descubierto después de la realización del hecho punible. Nuevamente, lo que el binomio Policía / Fiscalía deben hacer es identificar al responsable del delito pero la mera recepción de la llamada –o mensaje de texto, WhatsApp, etc.– no posibilita en sí su descubrimiento. Este es un círculo vicioso pues para emplear la geolocalización del dispositivo necesitaríamos haber localizado previamente al agente pues, de lo contrato, el agente no habría sido descubierto y, por lo tanto, no nos encontraríamos en un supuesto de flagrancia.

- Ni el agraviado ni otra persona y mucho menos un dispositivo audiovisual ha identificado al agente durante o inmediatamente después de la comisión del hecho delictivo. En consecuencia, no nos encontramos ante este supuesto de flagrancia por indicios.
- Finalmente, la presunción legal de flagrancia tampoco se da ya que el agente no ha sido encontrado con vestigios de la comisión del delito. ***Este supuesto se aplica cuando el agente ya fue identificado y ubicado por la Policía y, por tanto, puede ser detenido. En el caso de la geolocalización, no podemos decir que se encontró al agente, sino que podría ser encontrado si se accede a la ubicación del dispositivo y eso no es flagrancia.***

Para demostrar que recién estaremos en flagrancia si se encuentra al agente con vestigios del delito. Esto significa que cuando la Policía solicita la geolocalización aún no se encuentra en flagrancia ya que la figura procesal no puede legitimar acciones anteriores a su configuración.



Fuente: (Elías. R, 2016. p. 8)

La geolocalización sí permitiría encontrar al agente, incluso, dentro de las 24 horas de su comisión, pero no por encontrarse en un supuesto de flagrancia sino ante la comisión de un delito que merece ser investigado a través de búsqueda de pruebas con restricción de derechos, lo cual requiere autorización judicial previa.

Considerar que nos encontramos ***ante un delito flagrante sería restringir esta categoría procesal a la inmediatez temporal y prescindir de la inmediatez personal.*** Ello, sin duda, sería relajar las garantías procesales de todo ciudadano. ***Si se quiere invocar casuística, debemos tener presente que, de acuerdo a lo reportado por la Policía Nacional, el primer caso de empleo de geolocalización ante un (imposible) flagrante delito se trató de un "auto secuestro." El secuestro era una farsa. En***

consecuencia, tanto la Policía que solicitó y accedió como la operadora que brindó información, lesionaron derechos fundamentales de un ciudadano. (Elías. R, 2016. p. 8)

En segundo lugar, el Ejecutivo planteó la facultad legislativa como una propuesta excepcional para combatir casos de sicariato, extorsión, tráfico ilícito de drogas e insumos químicos, usurpación, tráfico de terrenos y tala ilegal de madera, pero la redacción del Decreto Legislativo permite solicitar la geolocalización, sin autorización judicial, de prácticamente cualquier delito previsto en el Código Penal. Si concordamos el artículo 6.2 con el artículo 1 del Decreto Legislativo tenemos que esta norma se aplica tanto a la delincuencia común como al crimen organizado; es decir, a todo el catálogo de delitos del Código Penal.

En vez de seleccionar un grupo específico de delitos en los que se podría aplicar la geolocalización, como el en caso de la interferencia de las comunicaciones, el Ejecutivo aprobó que sea aplicable a todos los ilícitos sancionados con pena superior a cuatro años de privación de libertad.

De este modo, los delitos que posibilitan la geolocalización sin autorización judicial no se reducen a aquellos catalogados como graves pues esta herramienta también podría emplearse ante casos de estafa, corrupción de funcionarios, fraude informático, fraude en la administración de personas jurídicas, ultraje a los símbolos patrios, y un largo etcétera.

Como puede apreciarse, al no existir una clara restricción, posibilita la ubicación en tiempo real de cualquier ciudadano que cuente con un dispositivo electrónico y que haya sido denunciado ante la Policía.

En tercer lugar, la norma exige que el acceso a los datos constituya un medio necesario para la investigación. Este extremo está relacionado con el sub-principio de necesidad que forma parte del principio constitucional de proporcionalidad, exigido cuando se deben adoptar acciones que restringen derechos fundamentales.

Siendo esto así, nos debemos preguntar: ¿a quién le corresponde realizar el análisis jurídico constitucional para la restricción de derechos en la búsqueda de pruebas? ¿A la Policía o a la Fiscalía?

Es la Constitución la que posibilita excepcionalmente que la Policía pueda realizar este tipo de actos, pero únicamente en dos casos concretos: detención (artículo 2.24.f Const.) y allanamiento (artículo 2.9 Const.). De esta manera, para la afectación al secreto de las comunicaciones, se requiere autorización judicial previa. El Decreto Legislativo no puede legitimar una restricción constitucional tan grave.

c) El Procedimiento inconstitucional que merma la función del fiscal en el conocimiento e investigación del delito.

Los artículos 4 y 5 del Decreto Legislativo regulan el procedimiento policial para acceder a la ubicación de los dispositivos electrónicos y el pedido de convalidación judicial. Los pasos que sigue este procedimiento especial y demostraremos que existen vicios: el sacrificio de garantías en aras de una supuesta eficacia investigativa.

vii. ***La unidad a cargo de la investigación policial***, una vez verificados los supuestos del artículo***, pone en conocimiento del Ministerio Público el hecho y formula el requerimiento a la unidad especializada de la Policía Nacional del Perú para efectos de la localización o geolocalización*** (artículo

4.1). *La norma condiciona la puesta en conocimiento de los hechos denunciados a una previa verificación a cargo de la Policía de los supuestos, que, impide tratar los delitos cometidos a través de dispositivos móviles bajo la figura de flagrancia delictiva. Dicho de otro modo, la redacción es tendenciosa pues,* ***de acuerdo al artículo 331.1 del Código Procesal Penal, la Policía debe de comunicar inmediatamente la denuncia formulada por un ciudadano ante su dependencia y no condicionarlo a la verificación previa de los referidos supuestos.*** (Elías. R, 2016)

viii. ***La unidad especializada de la Policía Nacional del Perú que recibe el requerimiento, previa verificación del responsable de la unidad solicitante, cursa el pedido a los concesionarios de los servicios públicos de telecomunicaciones o a entidades públicas relacionadas con este servicio, a través del correo electrónico institucional u otro medio idóneo convenido (artículo 4.2).*** Los argumentos por los que la Policía no tiene la facultad constitucional de solicitar datos de localización o geolocalización a las empresas de comunicación al encontrarse protegidas por el derecho fundamental del secreto de las comunicaciones. ***No se ha tenido acceso al protocolo que regula el procedimiento que estamos analizando; sin embargo, la Policía ya hace uso de esta facultad***. Se espera que todo el circuito de comunicación ***-desde el registro de la denuncia, la comunicación al Ministerio Público, así como a la Unidad Especializada, la verificación del responsable hasta los correos electrónicos de solicitud y de respuesta de las operadoras- se encuentre anexo a la carpeta fiscal*** pues, de lo contrario, se estaría restringiendo el derecho a la defensa ya que no tendría la posibilidad de verificar cómo se desarrolló el procedimiento. (Elías. R, 2016)

ix. Los concesionarios o servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, están obligados a brindar los datos de localización o geolocalización de manera inmediata, las veinticuatro (24) horas del día de los trescientos sesenta y cinco (365) días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento (artículo 4.3). Sé que el término "inmediato" aumenta los riesgos al condicionar la aplicación de esta facultad excepcional a casos de flagrancia.

Ejemplo.: El 1 de enero de 2016 a las 00:00 recibimos una llamada extorsionadora. Acudimos a la Policía a las 18:00, mientras se realizan las comunicaciones respectivas pasan algunas horas y la Unidad Especializada remite la comunicación a la operadora a las 23:00 y esta responde a las 01:00. A quienes aún consideren que sólo se requiere inmediatez temporal y no personal para la configuración de la flagrancia, la pregunta es ¿qué harían con la información recibida pues aun cuando encontrasen al agente? Al haber pasado más de 24 horas, este no podrías detenido. Es más, habrían recibido la información cuando la flagrancia (que se considera no se configura) ya habría cesado. (Elías. R, 2016)

x. La unidad a cargo de la investigación policial realiza las diligencias pertinentes en consideración de la información obtenida y a otras técnicas de investigación, sin perjuicio de lo establecido en el artículo 5 (artículo 4.4). ***Que la Policía realice actos de investigación no genera problema alguno, pues forman parte de sus funciones conforme se encuentra previsto en el artículo 67 del Código Procesal Penal.***, salvo detención policial o

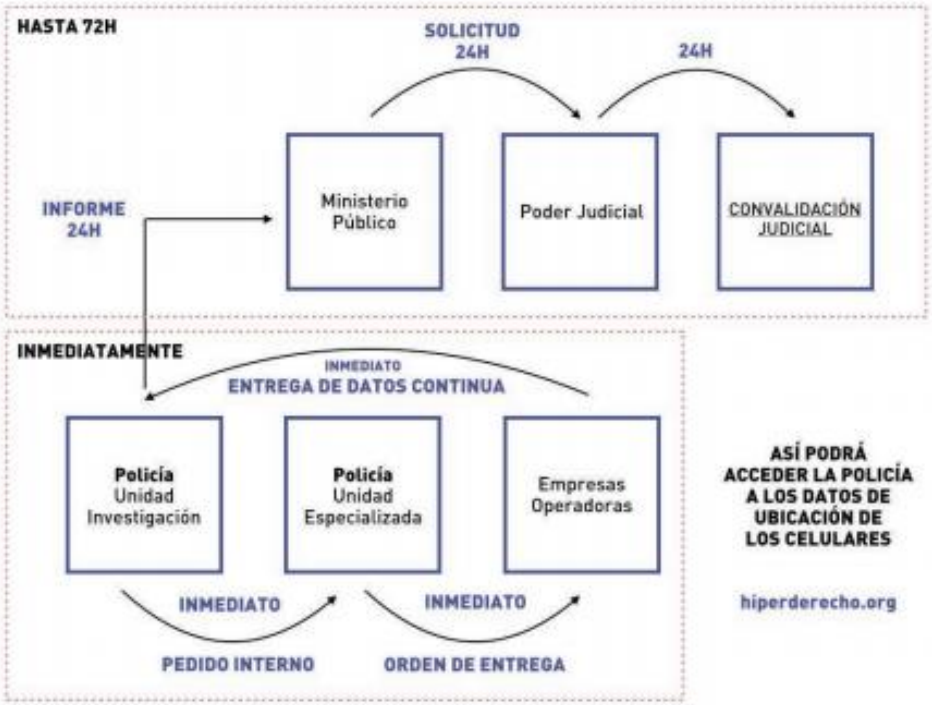
allanamiento en flagrancia, no está facultada constitucionalmente a restringir nuestro derecho al secreto de las comunicaciones. (Elías. R, 2016)

xi. La unidad policial a cargo de la investigación policial, dentro de las 24 horas de comunicado el hecho al Fiscal correspondiente, le remitirá un informe que sustente el requerimiento para su convalidación judicial (artículo 5.1***). El Fiscal dentro de las veinticuatro (24) horas de recibido el informe, solicita al Juez la convalidación de la medida (artículo 5.2). La redacción es inadecuada y sugiere que en todos los casos el Fiscal solicitará la convalidación judicial. Nuevamente, el titular de la acción penal es el Fiscal y, de acuerdo al artículo 60.2 del Código Procesal Penal: "El Fiscal conduce desde su inicio la investigación del delito. Con tal propósito la Policía Nacional está obligada a cumplir los mandatos del Ministerio Público en el ámbito de su función.***" En consecuencia, pese a que la norma no lo expresa, si el Fiscal no está de acuerdo con la solicitud de la Policía tiene toda la potestad de ordenar se deje sin efecto la medida. ***El problema surgirá cuando la Policía haya obtenido información relacionada a la localización o geolocalización y después la Fiscalía muestre su disconformidad con tal pedido: ¿qué sucede con la información?, ¿quién se responsabilizará por la lesión sufrida por el ciudadano afectado? Al no contar con el Protocolo de actuación (porque el Ejecutivo le ha conferido la condición de información reservada) no sabemos de qué forma la Fiscalía comunicaría la revocatoria de la solicitud policial a la operadora de telefonía: ¿directamente?, ¿a través de la Unidad Especializada de la Policía?, ¿a través de la Unidad de Investigación?*** (Elías. R, 2016)

xii. ***El juez competente resolverá mediante trámite reservado y de manera inmediata, teniendo a la vista los recaudos del requerimiento fiscal, en un plazo no mayor de 24 horas. La denegación del requerimiento deja sin efecto la medida y podrá ser apelada por el Fiscal. El recurso ante el juez superior se resolverá en el mismo plazo y sin trámite alguno (artículo 5.3). El juez que convalida la medida establecerá un plazo máximo que no excederá de sesenta (60) días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del Fiscal (artículo 5.4).***

Este último paso debió ser el segundo en el procedimiento –el primero, obviamente, sería la comunicación y solicitud a cargo del Fiscal–. Ya que toda norma es perfectible, consideramos que, en una eventual reforma, debería establecerse, al igual que en artículo 230 del Código Procesal Penal, que la resolución judicial debería indicar la información a la cual la Fiscalía puede acceder. Esto impedirá que la convalidación judicial sea tomada como un "cheque en blanco" que autoriza cualquier solicitud de información relacionada a la localización. Sin esta precisión, la Fiscalía o la Policía podrían solicitar ubicaciones históricas que no se encuentran vinculadas a la investigación criminal y, de este modo, lesionar el derecho a la intimidad personal. (Elías. R, 2016)

El siguiente flujograma explica gráficamente los pasos que, de acuerdo al Decreto Legislativo, sigue la Policía para acceder a nuestra localización o geolocalización. (Elías. R, 2016)



¿Qué pasa si la persona afectada acude directamente al Ministerio Público a denunciar, por ejemplo, una extorsión telefónica? Al no encontrarse acreditada o regulada normativamente, ¿la Fiscalía debería derivar el caso a la Unidad de Investigación Policial para que solicite, a su vez, que la Unidad Especializada de la Policía requiera a las empresas operadoras la ubicación del dispositivo electrónico?

Si esto es así, el procedimiento estaría siendo monopolizado por el Ejecutivo, a través de la Policía, desplazando a su vez al titular natural de la acción penal. (Elías. R, 2016)

d) El decreto Legislativo genera confusión de roles entre la Policía y el Ministerio Público.

De acuerdo al artículo IV del Código Procesal Penal, el Ministerio Público es el titular del ejercicio público de la acción penal y el encargado de conducir la investigación criminal desde el inicio. En consecuencia, “conduce y controla jurídicamente los actos de investigación que realiza la Policía Nacional.” el Decreto

Legislativo fue diseñado para que el pedido de información relacionado a la localización y geolocalización estuviese en control y monopolio del Poder Ejecutivo, a través de la Policía Nacional.

Un problema adicional que el Decreto Legislativo genera es la confusión de roles en la investigación criminal. Así, un logro obtenido con el Código Procesal Penal fue circunscribir las funciones de la Policía al plano operativo / forense y las funciones de la Fiscalía al plano jurídico.

Antes de la promulgación del referido Código, por ejemplo, ***la Policía tenía la facultad de calificar jurídicamente los hechos investigados bajo las figuras de atestado policial y parte policial.*** El primero se refiere a la calificación jurídica y atribución de responsabilidad al investigado, mientras que la segunda al reconocimiento contrario, es decir, a la falta de responsabilidad. (Elías. R, 2016)

Se sostiene que el Decreto Legislativo renueva esta confusión al exigir que sea el Policía y no el Fiscal quien valore jurídicamente si nos encontramos ante un supuesto de flagrancia de cualquier delito que sea sancionado con más de cuatro años en el Código Penal (el Ejecutivo no incorporó una lista taxativa de aplicación, sino empleó una fórmula general que no distingue entre tipos de delitos).

Hay que recordar que en el artículo 230 del Código Procesal Penal regula la intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles. Así, el numeral 4 de la norma en referencia precisa que:

> Los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta

> mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento. Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento. (Elías. R, 2016)

Por último, como puede apreciarse, un mismo supuesto de hecho (el acceso a la geolocalización de teléfonos móviles) ahora reviste dos mecanismos procesales: uno constitucional –exige resolución judicial previa– y uno inconstitucional –permite el acceso sin resolución judicial previa–, la flagrancia no valida el empleo del Decreto Legislativo

Entre los riesgos de la geolocalización se encuentran: "los seguimientos-trazabilidad de todo tipo de entidades (personas, animales, objetos), generación clandestina de perfiles-patrones (donde te encuentras, por donde te mueves, qué visitas, con quién te encuentras, cuánto tiempo estás, qué actividades haces, etc. vulnerando cuestiones relacionadas con la raza, política, religión, sexo, salud, etc.) para luego aplicarlos con herramientas de minería de datos (...) El geotagging permite conocer y señalar las coordenadas donde se encuentra una persona, casa (para robarla), se tomó una foto, bailamos, nos divertimos, hicimos negocios, restaurante, un lugar secreto, la localización de un evento, etc. pero como riesgo nos encontramos con la vigilancia social por GPS y la posibilidad que nos establezcan patrones de nuestros movimientos. Como contramedida sencilla frente al geotagging inhabilitar en el Smartphone o cámara de fotos (ya sea Android, iPhone o Blackberry) dicha característica que está activada por defecto"

4.2.2. Variable Derechos fundamentales vulnerados.

El derecho a la intimidad o a la vida privada involucra al conjunto de actos, situaciones o circunstancias que, por su carácter personalísimo, no se encuentran normalmente expuestos al dominio público. Protege tanto la intimidad de la persona como la de su familia, y comprende la libertad del individuo de conducirse en determinados espacios y tiempo, libre de perturbaciones ocasionadas por terceros, así como la facultad de defenderse de la divulgación de hechos priva.

El derecho a la intimidad se proyecta en dos dimensiones como secreto de la vida privada y como libertad. Concebida la intimidad como secreto, atentan contra ella todas las intromisiones o divulgaciones ilegítimas respecto a hechos relacionados con la vida privada o familiar, o las investigaciones también ilegítimas de acontecimientos propios de dicha vida. Concebida como libertad individual, la intimidad trasciende y se realiza en el derecho de toda persona a tomar por sí solas decisiones que conciernen a la esfera de su vida privada. (Elías. R, 2016)

La vulneración de la intimidad personal y familiar se produce por la sola intromisión externa o perturbación no autorizadas en las áreas privadas o reservadas (actos, hechos, hábitos, datos) que comprende, así como con las divulgaciones de su contenido sin contar con el consentimiento de su titular) (Rubio. M., 2013)

En el mismo sentido, el Tribunal Constitucional sostiene que: "(…) la vida privada se encuentra constituida por "los datos, hechos o situaciones desconocidas para la comunidad que, siendo verídicos, están reservados al conocimiento del sujeto mismo y de un grupo reducido de personas y cuya divulgación o conocimiento por otros trae aparejado algún daño" ***[STC 0009-2007-PI/TC y otros, fundamento 43]*** (Elías. R, 2016)

De esta forma, la intimidad se presenta como una libertad en sentido negativo, en tanto excluye o impide que terceros puedan acceder a determinados contenidos que la propia persona desea resguardar. (…) En el caso concreto de la intimidad, se demanda lo que en su momento la doctrina anglosajona denominó right to be alone, esto es, el derecho a no ser perturbado. La consecuencia natural del ejercicio de este ámbito del derecho a la intimidad es, que la persona tenga la posibilidad de tomar decisiones relacionadas con diversas áreas de la propia vida libremente, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el público. (Elías. R, 2016)

El concepto de intimidad tradicional debe ampliarse a fin de incorporar una nueva tutela del ciudadano, 24 que podría llamarse tutela al derecho de auto determinarse en una sociedad informativa (…) En lo personal, considero que podría discutirse si se trata de una efectiva ampliación del concepto tradicional o que el antes mencionado opera como un complemento de aquél, pero a todo evento, es clara la imposibilidad de quedarse atado a una concepción cristalizada en un momento anterior a la sociedad informatizada. (Riquert, M., 2003. p.51)

Las medidas que limitan derechos fundamentales, salvo las excepciones previstas en la Constitución, sólo podrán dictarse por la autoridad judicial, en el modo, forma y con las garantías previstas por la Ley. Se impondrán mediante resolución motivada, a iniciativa de la parte procesal legitimada. La orden judicial debe sustentarse en suficientes elementos de convicción, en atención a la naturaleza y finalidad de la medida y al derecho fundamental objeto de limitación, así como respetar el principio de proporcionalidad.

Hay que recordar, que los únicos supuestos en los que la Policía se encuentra facultada para restringir derechos fundamentales sin autorización judicial son: detención (artículo 2.24.f de la Constitución) y allanamiento (artículo 2.9 de la Constitución). En todos los demás casos, se requerirá resolución judicial motivada y que respete el principio de proporcionalidad constitucional.

Se afecta la intimidad por cuanto todas las personas tienen el derecho a defenderse de la divulgación de hechos privados. En un mundo globalizado e interconectado como el nuestro, ***¿acaso no tenemos el derecho a mantener en reserva el lugar donde nos encontramos o los que hemos visitado e, incluso, por dónde hemos deambulado?*** Piense el lector el trayecto que ha tenido el día de hoy, esta semana, este mes o este año, los lugares o las personas a las que visitó o con quienes se reunió***: ¿usted está de acuerdo que la Policía puede solicitar esta información sin autorización judicial?*** Este Decreto Legislativo no sólo permite localizarnos en tiempo real sino acceder a nuestra localización. En el Perú, algunos de los problemas asociados a esta política pública son:

- Afectan el derecho a la intimidad de todas las personas, aun las que no son investigadas por la comisión de delitos, pero que mantienen comunicación con personas investigadas. Pese a que las leyes actuales ordenan que las comunicaciones o las grabaciones que no sean necesarias para la investigación deben ser eliminadas, existen múltiples agentes a cargo de esta información, lo que aumenta el riesgo de fugas y la revelación por parte de terceros.

4.2.3. Variable Derecho Comparado.

En Paraguay también existen normas que regulan la intervención de las comunicaciones, lo que incluye no solo el acceso al contenido de las mismas sino

también a los metadatos. No obstante, respecto de los metadatos, en 2015 se quiso aprobar una regulación que permitía el acceso del tráfico IP de todos los ciudadanos a través de dispositivos móviles. A diferencia de Perú, en donde se pueden obtener todos los metadatos derivados de las comunicaciones, en el caso del proyecto paraguayo, solo se accedía al tráfico hecho a través de Internet (incluyendo los datos de geolocalización) y solo en los casos en que se estuvieran investigando los delitos de: Terrorismo, pedofilia y narcotráfico. Sin embargo, finalmente esta norma no prosperó y actualmente en Paraguay no existen normas similares a las que hay en Perú respecto al acceso a datos y metadatos sin orden judicial.

México presenta un caso similar a Perú pues en el año 2012 se realizó una reforma parcial de la Ley Federal de Telecomunicaciones y Radiodifusión, en la que se incluyeron varias disposiciones que permitían el acceso a los metadatos de geolocalización en tiempo real y sin mandato judicial previo. Estas normas actualmente se encuentran vigentes, aunque han recibido muchas críticas pues pese a que el acceso a estos metadatos está restringido a la investigación de ciertos tipos de delitos, el margen de discrecionalidad es alto.

A la luz de precedentes como la invalidación de la Directiva Europea de retención de datos, el fallido paso del proyecto de ley de retención en Paraguay, entre otros, queda claro que si bien el objetivo bajo el cual se gestan este tipo de leyes es legítimo, los mecanismos destinados a implementar las acciones pueden no serlo, llevando a la creación de situaciones de abuso que perjudican derechos fundamentales, rompiendo así el equilibrio que debe existir entre afectación y satisfacción de derechos.

Visto todo esto, urge modificar el Decreto Legislativo 1182 en los extremos que (i) permite el acceso sin autorización judicial de la Policía a la ubicación de cualquier

usuario de dispositivos móviles, y, (ii) ordena a las empresas de telecomunicaciones a conservar los datos derivados de las telecomunicaciones de sus usuarios por un período de tres años.

Finalmente, se muestra que en los diversos ordenamientos jurídicos se encuentra enmarcado en la norma penal, o normal especial.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES.

5.1. Conclusiones.

El Decreto Legislativo Afectan el derecho a la intimidad, debido a que hay personas que no son investigadas por la comisión de delitos, pero que mantienen comunicación con personas investigadas. Otorga facultad investigativa exclusivamente a una Unidad especializada de la Policía, desplazando incluso a la fiscalía.

Busca hacer que las partes que intervienen en el procedimiento cumplan a cabalidad sus responsabilidades, y de esa manera tener resultados óptimos en la administración de justicia.

Frente a una denuncia en cualquier comisaría, ésta pasará a la unidad especializada, quien a su vez comunica al fiscal, quien de manera inmediata verifica el delito flagrante, que la sanción del delito sea mayor de 4 años y que la geolocalización sea necesaria para la investigación.

Los procedimientos del decreto del decreto legislativo 1182 no se cumplen de manera adecuada, siendo estos ineficientes.

La legislación comparada regula el acto de investigación de geolocalización se encuentra enmarcada en la norma penal o norma especial, respaldando la facultad del efectivo PNP de hacer uso de la geolocalización sin autorización judicial.

5.2. Recomendaciones.

Recomendar a los estudiantes y profesionales del derecho hacer mayor hincapié y ahondar en temas relacionados con la geolocalización sin autorización judicial, establecido en el Decreto Legislativo 1182.

LISTA DE REFERENCIAS.

Abad, S. (2009). *El derecho al secreto de las comunicaciones*. Obtenido de Revistas.pucp.edu.pe: http://revistas.pucp.edu.pe/index.php/pensamientoconstitucional/article/download/2852/2780/.

Asociación de academías de la lengua española. (2015). *Diccionario panhispánico del español jurídico.* Panhispánico.

Asociación de Académias de la Lengua Española. (2009). *Real Académia Española.* Fundación La Caixa.

Badillo, J. Domingo, P. & Gonzales, I. (2018). *GPS. Derecho a la Circulación*. Obtenido de htt//www.topoequipos.com/dem/qu-es/terminolgiia/que-es--un.gps

Beltrán, G. (2015). *La Geolocalización Social.*

Bernejo, D. (2021). *Tecnologías de la información y comunicación (TIC)*. Obtenido de Economipedia: https://economipedia.com/definiciones/tecnologias-de-la-informacion-y-comunicacion-tic.html.

Caballero. V. (2015). *Todo lo que tienes que saber sobre la Nueva Ley Stalker, la Nueva Amenaza Digital contra tu Privacidad.* Obtenido de Utero.pe: http://utero.pe/2015/07/30/todo-lo-que-tienes-que-saber-sobre-la-nueva-ley-stalker-la-nueva-amenaza-digital-contra-tu-privacidad/

Cabellos. L. (2017). *Datos de Geolocalización como medida de investigación. Avances en el sistema Jurídico Procesal Penal*: Universidad Nacional de Educación a Distancia.

Obtenido de http://e-spacio.uned.es/fez/eserv/tesisuned:Derecho-Lmcabello/CABELLO_GIL_LauraMaria_Tesis.pdf

Campos. E. (2019). *Geolocalización del imputado en el Perú, por Edhin Campos Barranzuela*. Obtenido de Lp. Pasion por el Derecho: https://lpderecho.pe/geolocalizacion-imputado-peru/

Caro. D. (2015). *La Inconstitucionalidad de la Ley de Localización y Geolocalización*. Obtenido de Gestión: https://webcache.googleusercontent.com/search?q=cache:HSeOZzQdBnQJ:https://gestion.pe/opinion/inconstitucionalidad-ley-localizacion-geolocalizacion-96109-noticia/+&cd=2&hl=es&ct=clnk&gl=pe

Chipana, J & López J. (2019). *¿Se puede interceptar legalmente las comunicaciones que se hacen a través del WhatsApp?* Obtenido de La Ley. El ángulo Legal de la Noticia.: https://laley.pe/art/7013/la-interceptacion-legal-en-las-comunicaciones-app2app

Daccach, J. (2007). *Tecnologías de la Información y Comunicaciones (TICs)*. Obtenido de http_//www.gestiopolis.com/delta*term/TER434.html

Elías. R. (2016). *Decreto Legislativo 1182, Geolocalización y Proceso Penal. Sacrificio de Garantías en favor de una supuesta Eficacia Investigativa.* Hiperderecho.org. Obtenido de https://webcache.googleusercontent.com/search?q=cache:j1Zjh-9yDCkJ:https://hiperderecho.org/wp-content/uploads/2016/05/elias_geolocalizacion_proceso_penal.pdf+&cd=2&hl=es&ct=clnk&gl=pe

Fernández del Campo, I. (2015). *Los Servicios de Geolocalización y el Derecho a la Protección de Datos Personales*. Universidad de Salamanca. Obtenido de

https://gredos.usal.es/bitstream/handle/10366/127341/TG_FernandezdelCampo_Servicios.pdf?sequence=1

Flores. M. (2016). *La Geolocalización y el Derecho a la Privacidad. Análisis de la acción de la inconstitucionalidad 32/2012.* Universidad Nacional Autónoma de México. Obtenido de http://dx.doi.org/10.22201/25940082e.2016.1.10228

García. C y Enríquez. (s.f.). *Ley General de Protección de Datos Personlaes en Posesión de sujetos obligados.* México.

Gob. pe. (s.f.). *Policía Nacional del Perú*. Obtenido de https://www.gob.pe/4336-policia-nacional-del-peru-que-hacemos

Gómez. J. (2004). *Neurociencia coginitiva y Educación.* Chiclayo.

González, Hernández y Viña. (2014). *Cómo ser Mejor Estudiante*: Editorial Universitaria.

González. J. (2013). *Derechos Fundamentales afectados por la Geolocalización.* Obtenido de Derechos fundamentales afectados por la geolocalización.

Hernández, Fernández & Batista. (2010). *Metodología de la Investigación*: Mc Graw-Hill/Interamericana Editores. S.A.

Hiperderecho. (2015). *Contra el D.L. 1182.* Obtenido de https://hiperderecho.org/dl1182/

INFODF. (2015). *Principios internacionales sobre la aplicación de los Derechos Humanos a la Vigilancia de las comunicaciones.* Obtenido de http://www.infodf.org.mx/dp/doctos/15/27/13_Principios_EFF.pdf.

Iniseg. (2019). *¿Qúe es el crimen organizado y sus efectos en la seguridad?* Obtenido de Seguridad al día: https://www.iniseg.es/blog/seguridad/que-es-el-crimen-organizado-

y-sus-efectos-en-la-seguridad/#:~:text=Para%20explicarlo%20en%20palabras%20m%C3%A1s,cierta%20jerarqu%C3%ADa%2C%20roles%20y%20funciones.

La Ley. (2015). *¿Por qué es incostitucional la ley de Geolocalización?* La Ley. El ángulo Legal de la Noticia.

Lancaster. F y Pinto. M. (2010). *Procesamiento de la Información Científica*: la Muralla . Arco Libros.

López, J. (2015). *La Flagrancia Delictiva como instrumentoprocesal de lucha contra la criminalidad*. Obtenido de https://webcache.googleusercontent.com/: https://webcache.googleusercontent.com/search?q=cache:KhHi3ihAcY0J:https://www.mpfn.gob.pe/escuela/contenido/actividades/docs/4263_la_flagrancia_delictiva.pdf+&cd=1&hl=es&ct=clnk&gl=pe

Marcia, R. (2013). *Sanciones Penales en el Sistema Jurídico Peruano*. Obtenido de Revista Jurídica virtual Año III: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/7620EFA610E504C205257D270070381F/%24FILE/06ROSAS.pdf.

Martínez R. (2016). *Geolocalización: Entre el Bien Común y el Derecho a la Privacidad*. Asesores en Soluciones. Obtenido de http://asesoresensoluciones.com/index.php/geolocalizacion-entre-el-bien-comun-y-el-derecho-a-la-privacidad.

Masot, N. (2019). *Tecnologías de la información geográfica en el análisis epacial. Aplciaciones en los sectores púbicos empresarial y universitario.* Obtenido de Comunidad ISM: http://www.comunidadism.es/herramientas/tecnologias-de-la-

informacion-geografica-en-el-analisis-espacial#:~:text=Las%20Tecnolog%C3%ADas%20de%20la%20Informaci%C3%B3n,distintos%20como%20el%20medio%20ambiente

Ministerio de Cultura. (2002). *Centro de Documentación e investigación*.

Ministerio Público - Fiscalía de la Nación. (s.f.). *Fiscalia de la Nación*. Obtenido de https://www.mpfn.gob.pe/fiscaliadelanacion/#:~:text=La%20Fiscal%C3%ADa%20de%20la%20Naci%C3%B3n,la%20Fiscal%C3%ADa%20de%20la%20Naci%C3%B3n.

Mogrovejo. F. (2019). *El acceso a la Geolocalización por parte de la Policía sin orden Judicial"*. Universidad Nacional Federico Villarreal. Obtenido de http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/3355/MOGROVEJO%20RAMOS%20FREDDY%20%20ANGEL%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y

Neciosup. S. (2017). *Afectación de los Derechos Constitucionales por la Aplicación del Decreto Legislativo N° 1182 referido a la Lye de Geolocalización en su implicancia en la ciudad de Chiclayo*: Universidad Señor de Sipán. Obtenido de http://servicios.uss.edu.pe/bitstream/handle/uss/6767/NECIOSUP%20MINCHOLA%20STEPHANY%20YAMILETH.pdf?sequence=1&isAllowed=y

Omeba, E. (2005). *Referido que todo lo íntimo es necesariamente privado, pero no todo lo privado es necesariamente íntimo.*

Pasión por el Derecho. (2020). *Detención en cuasiflagrancia*. Obtenido de LEGIS : https://lpderecho.pe/tag/cuasiflagrancia/

Pick, S. y Velasco de la Fuente, A. (2002). *Como investigar en ciencias sociales*: Editorial Trillas.

Privacy International. (2015). *Información General sobre Privacidad*. Obtenido de https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes/informacion-general-sobre-privacidad

Puig, C y Valera A. (2008). *Tecnologías de la Información Geográfica*. Obtenido de Upcommons.upe.edu: https://upcommons.upc.edu/bitstream/handle/2099/7408/08_TIG_02_introduccion.pdf?sequence=1&isAllowed=y.

Rubio, C. (1999). *Estudio de la Constitución Política del Perú.* Lima: Fondo Editorial de la Pontificia Católica del Perú.

Ruiz. A. (2010). *Consideraciones acerca de la explosión geográfica: Geografía colaborativa e información geográfica voluntaria acreditada.* Geofocus.

Salazar, S. (2020). *¿Qué son ls interceptaciónes telefónicas y cuándo son ilegales?* Obtenido de https://colombiacheck.com/investigaciones/explicador-que-son-las-interceptaciones-telefonicas-y-cuando-son-ilegales

Salvador. E. (2018). *La Problemática de la protección de Datos Personales y la Geolocalización.* Ecuador: Universidad de las Americas. Obtenido de http://dspace.udla.edu.ec/bitstream/33000/10973/1/UDLA-EC-TAB-2018-53.pdf

Sánchez, E. (2008). *Las tecnologías de Información y comunicación (TIC) desde una perspectiva social*. Obtenido de Revista eletrónica Educare. Vol. XII. : https://www.redalyc.org/pdf/1941/194114584020.pdf

Significados. (2017). *Significados*. Obtenido de https://www.significados.com/delincuencia/#:~:text=La%20delincuencia%20com%C3%BAn%20es%20aquella,No%20son%20delincuentes%20especializados.

UPAGU. (2020). *Formato de redacción de la Universidad Privada Antonio Guillermo Urrelo: Facultad de Derecho y Ciencias Políticas.* revisado en: https://drive.google.com/file/d/1yuVgh6ZCu3EWs9f1oymjnC2Wt4QW3yhC/view

Wikipedia. (2017). *Aparato electrónico*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Aparato_electr%C3%B3nico

Wikipedia. (2017). *Derecho a la intimidad*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Derecho_a_la_intimidad

Wikipedia. (s.f.). *Sistema de Información Geográfica*. Obtenido de Wikipedia: https://es.wikipedia.org/wiki/Sistema_de_informaci%C3%B3n_geogr%C3%A1fica#T%C3%A9cnicas_utilizadas_en_los_sistemas_de_informaci%C3%B3n_geogr%C3%A1fica

Wikipedia. (2020). *Conectividad.*

Yupanqui. C. (2015). *Impacto del Decreto Legislativo N° 1182 en el Contendio esencial de los Derechos a la Información y Libertad de Expresión.* Lima: Universidad Autonoma del Perú. Obtenido de http://repositorio.autonoma.edu.pe/bitstream/AUTONOMA/462/1/Carlos%20Yupanqui.pdf

ANEXOS.

ANEXO 01. Solicitud de acceso a la información.

MANUAL DE DOCUMENTACION POLICIAL

FORMATO 69

SOLICITUD DE ACCESO A LA INFORMACION

FORMULARIO DE SOLICITUD DE ACCESO A LA INFORMACIÓN PÚBLICA
MINISTERIO DEL INTERIOR - POLICIA NACIONAL DEL PERÚ
(Por favor entregar en mesa de partes el original y copia incluyendo anexos)

PERÚ	MINISTERIO DEL INTERIOR POLICIA NACIONAL DEL PERÚ	SOLICITUD DE ACCESO A LA INFORMACIÓN PÚBLICA	N° DE REGISTRO
		Texto Único Ordenado de la Ley 27806 - Ley de Transparencia y Acceso a la Información Pública, aprobado por DS N° 043-2003-PCM	

I. FUNCIONARIO RESPONSABLE DE LA ATENCIÓN DE PEDIDOS EN EL MARCO DE LA LEY DE TRANSPARNCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

I. FUNCIONARIO RESPONSABLE DE LA ATENCIÓN DE PEDIDOS EN EL MARCO DE LA LEY DE TRANSPARNCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

II. DATOS DEL SOLICITANTE

APELLIDOS Y NOMBRES / RAZÓN SOCIAL	DOCUMENTO DE IDENTIDAD DNI/LM/CE/RUC/OTRO
DOMICILIO	

DOMICILIO

AV/CALLE/JR/PJE	N°/DPTO/INT	URBANIZACION	DISTRITO	PROVINCIA	DEPARTAMENTO

PROVINCIA	DEPARTAMENTO	CORREO ELECTRÓNICO

III. INFORMACIÓN SOLICITADA

PROVINCIA DEPARTAMENTO

CORREO ELECTRÓNICO

V. DEPENDENCIA DE LA CUAL SE REQUIERE LA INFORMACIÓN

VII. FORMA DE ENTREGA DE LA INFORMACIÓN (MARCA CON UNA "x")

COPIA SIMPLE ☐ DISKETTE ☐ CD ☐ CORREO ELECTRONICO ☐ OTROS ☐

APELLIDOS Y NOMBRES	FECHA Y HORA DE RECEPCIÓN
	FIRMA OBSERVACIONES
FIRMA	

OBSERVACIONES

ANEXO 2: Decreto Legislativo N° 1182.

DECRETO LEGISLATIVO

Nº 1182

El presidente de la republica

Por cuanto:

Que, mediante Ley Nº 30336 El congreso de la república ha delegado en el poder ejecutivo la facultad de legislar en materia de fortalecimiento de la seguridad ciudadana, lucha contra la delincuencia y el crimen organizado, por un plazo de noventa (90) días calendario;

Que, el literal a) del artículo 2 de la ley Nº 30336 faculta al poder ejecutivo para fortalecer la seguridad ciudadana, la lucha contra la delincuencia y el crimen organizado, en especial para combatir el sicariato, la extorsión, el tráfico ilícito de drogas e insumos químicos, la usurpación y tráfico de terrenos y la tala ilegal de madera;

Que, en el literal d) del artículo 2 de la citada ley faculta al poder ejecutivo para potenciar la capacidad operativa de la policía nacional del perú;

De conformidad con lo establecido en el artículo 104 de la Constitución Política del Perú;

DECRETO LEGISLATIVO

QUE REGULA EL USO DE LOS DATOS DERIVADOS DE LAS TELECOMUNICACIONES PARA LA IDENTIFICACIÓN, LOCALIZACIÓN Y GEOLOCALIZACIÓN DE EQUIPOS DE COMUNICACIÓN, EN LA LUCHA CONTRA LA DELINCUENCIA Y EL CRIMEN ORGANIZADO

Artículo 1.- Objeto
El presente decreto legislativo tiene por objeto fortalecer *las acciones de prevención, investigación y combate de la delincuencia común y el crimen organizado, a través del uso de tecnologías de la información y comunicaciones por parte de la policía nacional del Perú.*

Artículo 2.- Finalidad
La finalidad del presente decreto legislativo es regular el acceso de la unidad especializada de la Policía Nacional del Perú, en casos de flagrancia delictiva, a la localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar.

Artículo 3.- Procedencia
La unidad a cargo de la investigación policial solicita a la unidad especializada el acceso inmediato a los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar, siempre que concurran los siguientes presupuestos:

A. Cuando se trate de flagrante delito, de conformidad con lo dispuesto en el artículo 259 del decreto legislativo nº 957, código procesal penal.
B. Cuando el delito investigado sea sancionado con pena superior a los cuatro años de privación de libertad.
C. El acceso a los datos constituya un medio necesario para la investigación.

Artículo 4.- procedimiento
4.1 la unidad a cargo de la investigación policial, una vez verificados los supuestos del artículo precedente, pone en conocimiento del ministerio público el hecho y formula el requerimiento a la unidad especializada de la Policía Nacional del Perú para efectos de la localización o geolocalización.
4.2 la unidad especializada de la Policía Nacional del Perú que recibe el requerimiento, previa verificación del responsable de la unidad solicitante, cursa el pedido a los concesionarios de los servicios públicos de telecomunicaciones o a las entidades públicas relacionadas con estos servicios, a través del correo electrónico institucional u otro medio idóneo convenido.
4.3 los concesionarios de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, están obligados a brindar los datos de localización o geolocalización de manera inmediata, las veinticuatro (24) horas del día de los trescientos sesenta y cinco (365) días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento.
4.4 la unidad a cargo de la investigación policial realiza las diligencias pertinentes en consideración a la información obtenida y a otras técnicas de investigación, sin perjuicio de lo establecido en el artículo 5.

Artículo 5.- convalidación judicial
5.1 la unidad a cargo de la investigación policial, dentro de las 24 horas de comunicado el hecho al fiscal correspondiente, le remitirá un informe que sustente el requerimiento para su convalidación judicial.
5.2 el fiscal dentro de las veinticuatro (24) horas de recibido el informe, solicita al juez la convalidación de la medida.
5.3 el juez competente resolverá mediante trámite reservado y de manera inmediata, teniendo a la vista los recaudos del requerimiento fiscal, en un plazo no mayor de 24 horas. La denegación del requerimiento deja sin efecto la medida y podrá ser apelada por el fiscal. El recurso ante el juez superior se resolverá en el mismo plazo y sin trámite alguno.
5.4 el juez que convalida la medida establecerá un plazo que no excederá de sesenta (60) días. Excepcionalmente podrá prorrogarse por plazos sucesivos, previo requerimiento sustentado del fiscal.
Artículo 6.- exclusión y protección del secreto de las telecomunicaciones

El presente decreto legislativo está referido estrictamente a los datos de localización o geolocalización y se excluyen expresamente cualquier tipo de intervención de las telecomunicaciones, las que se rigen por los procedimientos correspondientes.

Artículo 7.- responsabilidades por uso indebido de los datos de localización o geolocalización
7.1 los denunciantes o el personal policial que realicen actos de simulación de hechos conducentes a la aplicación de la intervención excepcional de la unidad especializada de la Policía Nacional del Perú son pasibles de sanción administrativa, civil y penal según corresponda.
7.2 los que valiéndose de su oficio, posición, jerarquía, autoridad o cargo público induzcan, orienten o interfieran de algún modo en el procedimiento establecido en el artículo 4, son pasibles de sanción administrativa, civil y penal según corresponda.
7.3 los concesionarios de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, así como los que participan en el proceso de acceso a los datos de localización o geolocalización, están obligados a guardar reserva, bajo responsabilidad administrativa, civil y penal según corresponda.

Artículo 8.- exención de responsabilidad
Los concesionarios de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios están exentos de responsabilidad por el suministro de datos de localización o geolocalización, en el marco del presente decreto legislativo.

Artículo 9.- financiamiento
La implementación de las acciones correspondientes al pliego ministerio del interior previstas en el presente decreto legislativo, se financian con cargo al presupuesto institucional de dicho pliego, sin demandar recursos adicionales al tesoro público.

Disposiciones complementarias
Finales

Primera. - implementación
Para los efectos de la entrega de los datos de localización o geolocalización de teléfonos móviles o dispositivos electrónicos de naturaleza similar, los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas o privadas relacionadas con estos servicios, implementan mecanismos de acceso exclusivo a la unidad especializada de la Policía Nacional del Perú.

Segunda. - conservación de los datos derivados de las telecomunicaciones
Los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas relacionadas con estos servicios deben conservar los datos derivados de las telecomunicaciones durante los primeros doce (12) meses en sistemas informáticos que permitan su consulta y entrega en línea y en tiempo real. Concluido el referido periodo, deberán conservar dichos datos por veinticuatro (24) meses adicionales, en un sistema de almacenamiento electrónico.

La entrega de datos almacenados por un periodo no mayor a doce meses, se realiza en línea y en tiempo real después de recibida la autorización judicial. Para el caso de los datos almacenados por un periodo mayor a doce meses, se hará entrega dentro de los siete (7) días siguientes a la autorización judicial, bajo responsabilidad.

Tercera. - auditoría operativa
La inspectoría general del ministerio del interior y la inspectoría general de la Policía Nacional del Perú realizarán auditorías operativas relacionadas con el cumplimiento del presente decreto legislativo.

Cuarta. - contraloría general de la república
La contraloría general de la república, a través del órgano de control institucional y en el marco del sistema nacional de control, vela por el adecuado cumplimiento de lo dispuesto en el presente decreto legislativo.

Quinta. - mecanismos de advertencia y reporte de datos
Los concesionarios de servicios públicos de telecomunicaciones implementarán mecanismos de advertencia al destinatario de una comunicación producida desde un establecimiento penitenciario o de inmediaciones a este, a través de un mensaje previo indicando esta circunstancia.

Los concesionarios de servicios públicos de telecomunicaciones comunicarán a la unidad especializada el reporte de los datos identificatorios de teléfonos móviles o dispositivos electrónicos de naturaleza similar cuyas llamadas proceden de establecimientos penitenciarios.

Sexta. - infracciones y sanciones relativas a empresas operadoras
El ministerio de transportes y comunicaciones y el organismo regulador de las telecomunicaciones (Osiptel), mediante decreto supremo, establecerán las infracciones y sanciones aplicables a los sujetos obligados a brindar acceso a datos derivados de telecomunicaciones, por el incumplimiento de las obligaciones establecidas en la presente norma y su reglamento.

Disposiciones complementarias transitorias

Primera. - plazos para la implementación
En un plazo no mayor de treinta (30) días la unidad especializada de la Policía Nacional del Perú en coordinación con los concesionarios de servicios públicos de telecomunicaciones y con el apoyo técnico de la dirección ejecutiva de tecnología de información y comunicaciones de la Policía Nacional del Perú, podrán elaborar protocolos para el mejor acceso de los datos de localización o geolocalización.

En un plazo no mayor de treinta (30) días, a partir de la emisión de los citados protocolos, los concesionarios de servicios públicos de telecomunicaciones y las entidades públicas o privadas relacionadas con estos servicios y la unidad especializada con apoyo técnico de la dirección ejecutiva de tecnología de información y comunicaciones de la Policía Nacional del Perú diseñarán e implementarán las herramientas tecnológicas necesarias que viabilicen la aplicación de la presente norma.

Segunda. - fortalecimiento de la unidad especializada de la Policía Nacional del Perú
El ministerio del interior en un plazo no mayor de treinta (30) días, proporcionará los recursos logísticos y económicos, para el fortalecimiento de la unidad especializada de la Policía Nacional del Perú.

La Policía Nacional del Perú dotará del personal calificado necesario a la unidad especializada para el mejor cumplimiento de sus funciones e implementará un procedimiento especial de selección que incluirá la entrevista personal, exámenes toxicológicos y psicológicos, así como la prueba del polígrafo. Dicho personal estará sujeto a evaluación permanente.

La dirección ejecutiva de educación y doctrina de la Policía Nacional del Perú establece cursos de capacitación, especialización y perfeccionamiento para el personal de la unidad especializada a la que se refiere el presente decreto legislativo.

Disposiciones complementarias modificatorias

Primera. - modificación del artículo 162 del código penal
Modifíquese el artículo 162 del código penal, el cual en adelante tendrá la siguiente redacción:

"*artículo 162. Interferencia telefónica*
El que, indebidamente, interviene o interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años.
La pena privativa de libertad será no menor de diez ni mayor de quince años:
1. *Cuando el agente tenga la condición de funcionario o servidor público, y se impondrá además la inhabilitación conforme al artículo 36, incisos 1, 2 y 4.*
2. *Cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la ley 27806, ley de transparencia y acceso a la información pública.*
3. *Cuando el delito comprometa la defensa, seguridad o soberanía nacionales.*
Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Segunda. - incorporación del artículo 162-a al código penal
Incorpórese el artículo 162-a al código penal, con la siguiente redacción:

"artículo 162-a. Posesión o comercialización de equipos destinados a la interceptación telefónica o similar
El que fabrica, adquiere, introduce al territorio nacional, posee o comercializa equipos o softwares destinados a interceptar ilegalmente las comunicaciones o similares, será reprimido con pena privativa de la libertad no menor de diez ni mayor de quince años."

Tercera. - modificación del artículo 222 – a al código penal
Modifíquese el artículo 222-a del código penal, el cual en adelante tendrá la siguiente redacción:

"*artículo 222-a.- penalización de la clonación o adulteración de terminales de telecomunicaciones*
Será reprimido con pena privativa de libertad no menor de cuatro (4) ni mayor de seis (6) años, con sesenta (60) a trescientos sesenta y cinco (365) días multa, el que altere, reemplace, duplique o de cualquier modo modifique un número de línea, o de serie electrónico, o de serie mecánico de un terminal celular, o de imei electrónico o físico de modo tal que pueda ocasionar perjuicio al titular, al usuario del mismo, a terceros o para ocultar la identidad de los que realizan actos ilícitos."

Cuarta. - modificación del artículo 368 – a al código penal
Modifíquese el artículo 368-a del código penal, el cual en adelante tendrá la siguiente redacción:

"artículo 368-a.- ingreso indebido de equipos o sistema de comunicación, fotografía y/o filmación en centros de detención o reclusión
El que indebidamente ingresa, intenta ingresar o permite el ingreso a un centro de detención o reclusión, equipos o sistema de comunicación, fotografía y/o filmación o sus componentes que permitan la comunicación telefónica celular o fija, radial, vía internet u otra análoga del interno, así como el registro de tomas fotográficas, de video, o proporcionen la señal para el acceso a internet desde el exterior del establecimiento penitenciario será reprimido con pena privativa de libertad no menor de cuatro ni mayor de seis años.
Si el agente se vale de su condición de autoridad, abogado defensor, servidor o funcionario público para cometer o permitir que se cometa el hecho punible descrito, la pena privativa será no menor de seis ni mayor de ocho años e inhabilitación, conforme al artículo 36, incisos 1 y 2, del presente código."
Mando se publique y cumpla, dando cuenta al congreso de la república.

Dado en la casa de gobierno, en lima, a los veintiséis días del mes de julio del año dos mil quince.

Ollanta humala tasso

Presidente de la república

Pedro cateriano bellido

Presidente del consejo de ministros

José luis pérez guadalupe

Ministro del interior

Gustavo adrianzén olaya

ANEXO 03. Ejemplo de un Informe emitido por FRENPOL-CAJ-DIVINCRI-DEPINCRI-ARESE-SCG, durante el año 2019 en el Distrito de Cajamarca.

INFORME Nº 030-2019-SCG-FRENPOL-CAJ/DIVINCRI-DEPINCRI-ARESE.

Asunto	:	Resultado de las investigaciones, con conocimiento de la RMP. B. B. A O – Fiscal Adjunta Provincial de la 3ra. Fiscalía Provincial Penal Corporativa de Cajamarca, con relación a la denuncia formulada por E. L J (41), identificado con DNI N° XXXXXXXX, por la presunta comisión del Delito Contra el Patrimonio – Extorsión, en su agravio, cometido por "sujetos en proceso de identificación plena", hecho ocurrido el día 18SET2020, en el horario de 11.30 a 12.58 apróx., en esta ciudad de Cajamarca.
Competencia	:	- Tercera Fiscalía Provincial Penal Corporativa Cajamarca. Abogada. B. B. A. O. – Fiscal.
Referencia	:	- Acta de Denuncia N° 039 – 2019., del 18SET2019.
Investigados	:	- Sujetos en Proceso de Identificación Plena.

I. INFORMACIÓN

A. DENUNCIA POLICIAL

--- En la ciudad de Cajamarca, siendo las 11.40 horas del 19SET19, presente ante este departamento de investigación criminal la persona de E. ..P. (41); natural de Cajamarca - Cajamarca, nacido el 02SET1979, hijo de don José Ignacio L. S. y doña M. N. J. CH.; estado civil conviviente con J.P. C., grado de instrucción secundaria completa, técnico en automotriz, ocupación transportista de alimentos de primera necesidad y otros, en el trayecto de la ciudad de Cajamarca a Trujillo y viceversa, domiciliado en el Caserío Huambocancha Baja - Cajamarca, con teléfono nro. 976 XXX XXX (CLARO), quien con conocimiento del jefe del DEPINCRI y del representante del ministerio público de turno abogada B. A. O.- fiscal de la 3ra. FPPC - caj., denuncia que: el día 18SET2019, en el horario de 11.30 a 12.58, en circunstancias que se encontraba transitando por la vía de evitamiento norte, momento en el cual recibió cinco (05) llamadas del abonado N° 928 XXX XXX, de las cuales tres no ha respondido y en las dos otras llamadas una persona de sexo masculino le ha manifestado "E. L. P. están pagando para sacarte del negocio, no sé en qué problemas te has metido, pero si me das S/. 10 000.00 soles, yo te puedo cuidar mejor y ya no atentare en contra de tu vida y la de tu familia", además del mismo N° 928 XXX XXX, le han enviado cuatro mensajes de texto, en los que le indican que todo lo que le ha manifestado durante la llamada lo cumplirá, motivo por el cual se presentó ante esta dependencia policial para los fines correspondientes. siendo las 11.48 horas del mismo día se da por concluida la

presente, firmando e imprimiendo su huella digital en señal de conformidad el denunciante en presencia de instructor que certifica. --

II. DILIGENCIAS POLICIALES EFECTUADAS

A. Comunicación a la Autoridad Competente

- Vía telefónica al N° 983 XXX XXX, perteneciente a la Fiscalía Penal de Turno se hizo de conocimiento a la Abogada. B. B. A. O. – Fiscal Adjunta Provincial de la Tercera Fiscalía Provincial Penal Corporativa de Cajamarca, la denuncia realizada por E. L. J.(41), identificado con DNI N° XXXXXXXX, por la presunta comisión del Delito Contra el Patrimonio – Extorsión, en su agravio, cometido por "sujetos en proceso de identificación plena", hecho ocurrido el día 18SET2020, en el horario de 11.30 a 12.58 apróx., en esta ciudad de Cajamarca.

- Posteriormente se remitió vía WhatsApp a numero personal de la RMP. a cargo de la presente investigación, el Of. N° 2442-2019-SCG-FP-CAJ/DIVINCRI-DEPINCRI-AS., haciendo de conocimiento el presente caso.

B. ACTAS LEVANTADAS

Durante la investigación policial, se levantaron las actas siguientes:

1. De Denuncia Verbal:

--- Formulada el 19SET2019, a las 11.40 horas, por personal PNP perteneciente a la Oficina de Investigación de Secuestros y Extorsiones, de este DEPINCRI – DIVINCRI PNP – CAJ., a E. L.J. (41), identificado con DNI N° XXXXXXXX, por la presunta comisión del Delito Contra el Patrimonio – Extorsión, en su agravio, cometido por "sujetos en proceso de identificación plena", hecho ocurrido el día 18SET2019, en el horario de 11.30 a 12.58 apróx., en esta ciudad de Cajamarca.

2. <u>De Visualización de Equipo Celular:</u>

--- Formulada el 19SET2019, a las 11:55 horas, por personal PNP perteneciente a la Oficina de Investigación de Secuestros y Extorsiones, de este DEPINCRI – DIVINCRI PNP – CAJ., mediante la cual se visualizó las llamadas y mensajes de contenido extorsivo en el equipo móvil de propiedad del denunciante E. L. J. (41), identificado con DNI N° XXXXXXXX.

C. OFICIOS SOLICITADOS

1. OFICIO Nro. 2443-2019-FRENPOL-CAJ/DIVINCRI-DEPINCRI-AS, al Comandante PNP Jefe de la Unidad Especial en Geolocalización DIVINDAT PNP LIMA., solicitando la Identificación, Localización y Geolocalización de Equipo Móvil N° 928 XXX XXX, por encontrarse inmerso en la investigación materia del presente.

D. DOCUMENTOS RECEPCIONADOS

1. Procedente de la Unidad Especial en Geolocalización DIVINDAT PNP LIMA., se recepcionó el Of. N° 1270-2020-DIRINCRI-PNP/DIVINDAT-DEPGEO., de fecha 19SET2020, en el cual se indica que, en la fecha de lo solicitado resulta NO FACTIBLE por encontrase fuera de flagrancia delictiva.

E. DECLARACIONES RECEPCIONADAS

1. **E.L.J. – (DENUNCIANTE).**

III. ANALISIS Y EVALUACION DE LOS HECHOS

1. Como es de conocimiento del Ministerio Publico, el día 19SET2019, a horas 11:40, se apersono a este DEPINCRI PNP –CAJ., la persona de E.L.J. (41), identificado con DNI N° XXXXXXXX, con la finalidad de denunciar la presunta comisión del Delito Contra el Patrimonio – Extorsión, en su agravio, cometido por "sujetos en proceso de identificación plena", hecho ocurrido el día 18SET2019, en el horario de 11.30 a 12.58 apróx., en esta ciudad de Cajamarca.

2. A mérito de lo que antecede, se recabo la declaración del denunciante, de cuyo análisis se concluye que, el día 18SET2019, en el horario de 11.30 a 12.58, en circunstancias que se encontraba transitando por la vía de Evitamiento Norte – Cajamarca, recibió cinco (05) llamadas del abonado N° 928 XXX XXX, de las cuales tres no ha respondido y en las otras dos (02) llamadas una persona de sexo masculino le ha manifestado " E.L.J. r están pagando para sacarte del negocio, no sé en qué problemas te has metido, pero si me das S/. 10 000.00 soles, yo te puedo cuidar mejor y ya no atentare en contra de tu vida y la de tu familia", además del mismo N° 928 XXX XXX, le han enviado cuatro mensajes de texto, en los que le indican que todo lo manifestado durante la llamada lo cumplirá.

3. Dada esta situación, personal del Area de Secuestro y Extorsiones de esta DEPINCRI PNP – CAJ., de inmediato cumplio con requerir ante la Unidad PNP de Localización y Geolocalización Lima, la ubicación de la linea movil N° 928 XXX XXX, obteniéndose el Of. N° 1270-2020-DIRINCRI-PNP/DIVINDAT-DEPGEO., de fecha 19SET2019, en el cual se indica que, en la fecha de lo solicitado resulta NO FACTIBLE por encontrase fuera de flagrancia delictiva.

4. Asimismo, se hace de conocimiento de su Despacho, que hasta la formulación del presente documento, el agraviado E.L.J. (41), no se apersona a esta DEPINCRI PNP – CAJAMARCA, a comunicar que ha vuelto a recibir llamadas o mensajes con contenido extorsivo del N° 928 XXX XXX u otros, pese a las llamadas telefónicas realizadas por el instructor del presente caso, por lo que se podría inferir que dichas llamadas telefónicas únicamente fueron para intimidar al agraviado para realizar depósitos de dinero, asimismo, se ha desplegado diversas acciones relacionadas a la búsqueda de información en la jurisdicción de Cajamarca, respecto a la denuncia en curso, sin embrago, no se ha obtenido resultados favorables, no habiendo sido posible identificar

al autor (es) hasta la fecha, se continuará realizando diversas diligencias, cuyo resultado positivo se informara oportunamente.

5. Sin embargo, se sugiere al titular de la investigación, gestionar ante el órgano jurisdiccional competente la Medida Limitativa de Derecho – Levantamiento del Secreto de las Comunicaciones de la línea móvil N° 928 XXX XXX, a efectos de conocer al titular de esta línea móvil, reportes de llamadas, mensajes, ubicación de celdas activas, lo cual nos permitirá tener una apreciación coherente desde el punto de vista técnico y consecuentemente proceder conforme a ley.

IV. ANEXOS

- Un (01) Acta de Denuncia Verbal N° 349-2019.
- Una (01) Declaración de E.L.J..
- Un (01) Acta de Visualización de Equipo Celular.
- Un (01) Oficio N° 1270-2019-DIRINCRI-PNP/DIVINDAT-DEPGEO.
- Una (01) Copia xerográfica del DNI N° XXXXXXXX

Cajamarca, 29 setiembre de 2019.

ES CONFORME **INSTRUCTOR**

Anexo 04.Proyecto de ley N° 5091/2020 CR (Irrelevante en este informe de tesis)

<u>Dicho Proyecto al no ser aprobado no es considerado para esta investigación. Caso distinto si se aprueba tal proyecto es conveniente considerar las modificaciones realizadas para realizar una nueva investigación.</u>

CONGRESO REPÚBLICA

G.P. PODEMOS PERÚ

Decenio de la Igualdad de Oportunidades para Mujeres y Hombres
Año de la Universalización de la Salud

Proyecto de Ley Nº 5091/2020-CR

CONGRESO DE LA REPÚBLICA
AÑO DE TRAMITE CONSOLIDACION DE DOCUMENTOS
28 AGO 2020
RECIBIDO
Firma..... Hora.....

PROYECTO DE LEY QUE MODIFICA LOS ARTÍCULOS 2, 3 Y 4 DEL DECRETO LEGISLATIVO Nº 1182 QUE REGULA EL USO DE LOS DATOS DERIVADOS DE LAS TELECOMUNICACIONES PARA LA IDENTIFICACIÓN, LOCALIZACIÓN Y GEOLOCALIZACIÓN DE EQUIPOS DE COMUNICACIÓN, EN LA LUCHA CONTRA LA DELINCUENCIA Y EL CRIMEN ORGANIZADO

Los Congresistas de la República firmantes de conformidad con el artículo 107 de la Constitución Política del Perú y los artículos 75 y 76 del Reglamento del Congreso de la República, proponen el siguiente proyecto de ley:

EL CONGRESO DE LA REPÚBLICA;
Ha dado la Ley siguiente:

FÓRMULA LEGAL

PROYECTO DE LEY QUE MODIFICA LOS ARTÍCULOS 2, 3 Y 4 DEL DECRETO LEGISLATIVO Nº 1182 QUE REGULA EL USO DE LOS DATOS DERIVADOS DE LAS TELECOMUNICACIONES PARA LA IDENTIFICACIÓN, LOCALIZACIÓN Y GEOLOCALIZACIÓN DE EQUIPOS DE COMUNICACIÓN, EN LA LUCHA CONTRA LA DELINCUENCIA Y EL CRIMEN ORGANIZADO.

Artículo Único. Modificación de los artículos 2, 3 inciso a. y 4 inciso 4.3 del Decreto Legislativo Nº 1182 que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado.

Modifícanse los artículos 2; 3 inciso a. y 4 inciso 4.3 del Decreto Legislativo N° 1182, que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado, conforme al texto siguiente:

> **"Artículo 2.- Finalidad**
> La finalidad del presente decreto legislativo es regular el acceso de la unidad especializada de la Policía Nacional del Perú, en casos de flagrancia delictiva o ***en investigaciones preliminares por el delito contra la vida, el cuerpo y la salud; el delito contra la libertad, el delito contra el patrimonio y los delitos comprendidos en la Ley de Crimen Organizado,*** a la localización, geolocalización ***o rastreo*** de los teléfonos móviles ***y/o de cualquier otro dispositivo electrónico de comunicación.***

Artículo 3.- Procedencia

La unidad a cargo de la investigación policial solicita a la unidad especializada el acceso inmediato a los datos de localización, geolocalización ***o rastreo*** de los teléfonos móviles ***y/o de cualquier otro dispositivo electrónico de comunicación,*** siempre que concurran los siguientes presupuestos:

a. Cuando se trate de flagrante delito, de conformidad con lo dispuesto en el artículo 259 del Decreto Legislativo Nº 957, Código Procesal Penal o ***investigaciones preliminares por el delito contra la vida, el cuerpo y la salud; el delito contra la libertad, el delito contra el patrimonio y los delitos comprendidos en la Ley de Crimen Organizado.***

(...).

Artículo 4.- Procedimiento

(...)

4.3 Los concesionarios de servicios públicos de telecomunicaciones o las entidades públicas relacionadas con estos servicios, están obligados a brindar los datos de localización o geolocalización de manera inmediata ***y oportuna, dentro de un plazo máximo de*** veinticuatro (24) horas ***de solicitada la información por la Unidad Especializada de la Policía Nacional del Perú, cuya atención del requerimiento será*** las veinticuatro (24) horas del día de los trescientos sesenta y cinco (365) días del año, bajo apercibimiento de responsabilidades ***de carácter administrativo, civil y penal, en caso su incumplimiento***.(...)"

Disposición Complementaria Final

Única.- Para efectos de la presente Ley entiéndase que toda mención a los datos de localización, geolocalización o rastreo de los teléfonos móviles y/o de cualquier otro dispositivo electrónico de comunicación, tiene como finalidad la eficacia en la ubicación del equipo o lugar donde se cometen o generen los delitos y/o crimen organizado.

Robinson Gupioc Ríos

DANIEL URRESTI (AUTOR)

LUIS FELIPE CASTRO OLIVA

JOSE LUNA M.

J. Flores V.