Universidad Continental

FACULTAD DE DERECHO

Escuela Académico Profesional de Derecho

Tesis

Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático

Carlos Andre Blancas Quispialaya

Para optar el Título Profesional de Abogado

Huancayo, 2024

Universidad Continental

INFORME DE CONFORMIDAD DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

A	:	Decana de la Facultad de Derecho
DE	:	Ever Bello Merlo Asesor de trabajo de investigación
ASUNTO	:	Remito resultado de evaluación de originalidad de trabajo de investigación
FECHA	:	16 de Mayo de 2024

Con sumo agrado me dirijo a vuestro despacho para informar que, en mi condición de asesor del trabajo de investigación:

Título:
LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES EN SU FORMA DE INFORMACIÓN HISTÓRICA EN EL DELITO DE FRAUDE INFORMÁTICO

Autor:
Carlos Andre Blancas Quispialaya – EAP. Derecho

Se procedió con la carga del documento a la plataforma "Turnitin" y se realizó la verificación completa de las coincidencias resaltadas por el software dando por resultado 20 % de similitud sin encontrarse hallazgos relacionados a plagio. Se utilizaron los siguientes filtros:

- Filtro de exclusión de bibliografía — SI [X] NO [ ]
- Filtro de exclusión de grupos de palabras menores — SI [X] NO [ ]
  Nº de palabras excluidas **(en caso de elegir "SI")**: 16
- Exclusión de fuente por trabajo anterior del mismo estudiante — SI [X] NO [ ]

En consecuencia, se determina que el trabajo de investigación constituye un documento original al presentar similitud de otros autores (citas) por debajo del porcentaje establecido por la Universidad Continental.

Recae toda responsabilidad del contenido del trabajo de investigación sobre el autor y asesor, en concordancia a los principios expresados en el Reglamento del Registro Nacional de Trabajos conducentes a Grados y Títulos – RENATI y en la normativa de la Universidad Continental.

Atentamente,

_____
Asesor de trabajo de investigación
Ever Bello Merlo

Universidad Continental

DECLARACIÓN JURADA DE AUTORÍA

El presente documento tiene por finalidad declarar adecuada y explícitamente el aporte de cada autor en la elaboración del trabajo de investigación:

Título:
LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES EN SU FORMA DE INFORMACIÓN HISTÓRICA EN EL DELITO DE FRAUDE INFORMÁTICO

Yo: Carlos Andre Blancas Quispialaya – EAP. Derecho.

Declaro bajo juramento:

1. El trabajo de investigación es de mi autoría, dado que he participado en la ideación del problema, recolección de datos, elaboración y aprobación final del trabajo de investigación.
2. El trabajo de investigación no ha sido plagiado ni total ni parcialmente, para la cual se han respetado las normas internacionales de citas y referencias para las fuentes consultadas, por lo que no atenta contra derechos de terceros.
3. El trabajo de investigación es original e inédito, y no ha sido realizado, desarrollado o publicado, parcial ni totalmente, por terceras personas naturales o jurídicas. No incurre en autoplagio; es decir, no fue publicado ni presentado de manera previa para conseguir algún grado académico o título profesional.
4. Los datos presentados en los resultados son reales, pues no son falsos, duplicados, ni copiados, por consiguiente, constituyen un aporte significativo para la realidad estudiada.

De identificarse fraude, falsificación de datos, plagio, información sin cita de autores, uso ilegal de información ajena, falta de probidad académica, asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a las acciones legales pertinentes.

16 de mayo de 2024

_____
Firma
Carlos Andre Blancas Quispialaya

LEVANTAMIENTO DEL SECRETO DE LAS COMUNICACIONES EN SU FORMA DE INFORMACIÓN HISTÓRICA EN EL DELITO DE FRAUDE INFORMÁTICO

INFORME DE ORIGINALIDAD

20%	21%	5%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	5%
2	repositorio.ucv.edu.pe Fuente de Internet	3%
3	qdoc.tips Fuente de Internet	1%
4	idoc.pub Fuente de Internet	1%
5	repositorio.uss.edu.pe Fuente de Internet	1%
6	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
7	Submitted to Universidad Nacional de San Cristóbal de Huamanga Trabajo del estudiante	1%
8	tesis.ucsm.edu.pe Fuente de Internet	1%

9	doku.pub Fuente de Internet	<1 %
10	Submitted to Universidad Continental Trabajo del estudiante	<1 %
11	tesis.usat.edu.pe Fuente de Internet	<1 %
12	portalrevistas.aulavirtualusmp.pe Fuente de Internet	<1 %
13	repositorio.uladech.edu.pe Fuente de Internet	<1 %
14	Marco Urgell, Anna, Universitat Autònoma de Barcelona. Departament de Ciència Política i de Dret Públic. "La Intervención de las comunicaciones telefónicas : grabación de las conversaciones propias, hallazgos casuales y consecuencias jurídicas derivadas de la ilicitud de la injerencia /", Bellaterra : Universitat Autònoma de Barcelona,, 2010 Fuente de Internet	<1 %
15	www.tesisenred.net Fuente de Internet	<1 %
16	kerwa.ucr.ac.cr Fuente de Internet	<1 %
17	repositorioacademico.upc.edu.pe Fuente de Internet	<1 %

18	www.aulavirtualusmp.pe Fuente de Internet	<1 %
19	dokumen.pub Fuente de Internet	<1 %
20	renati.sunedu.gob.pe Fuente de Internet	<1 %
21	Submitted to usmp Trabajo del estudiante	<1 %
22	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1 %
23	Submitted to Universidad Peruana Los Andes Trabajo del estudiante	<1 %
24	docslide.us Fuente de Internet	<1 %
25	repositorio.upeu.edu.pe Fuente de Internet	<1 %
26	lpderecho.pe Fuente de Internet	<1 %
27	repositorio.unc.edu.pe Fuente de Internet	<1 %
28	idoc.tips Fuente de Internet	<1 %
29	www.lawandtrends.com	

	Fuente de Internet	<1 %
30	www.scribd.com Fuente de Internet	<1 %
31	digibug.ugr.es Fuente de Internet	<1 %
32	www.pj.gob.pe Fuente de Internet	<1 %
33	dspace.unitru.edu.pe Fuente de Internet	<1 %
34	www.informatica-juridica.com Fuente de Internet	<1 %
35	www.peruweek.pe Fuente de Internet	<1 %
36	prezi.com Fuente de Internet	<1 %
37	repositorio.unfv.edu.pe Fuente de Internet	<1 %
38	Submitted to Universidad Catolica de Avila Trabajo del estudiante	<1 %
39	documentop.com Fuente de Internet	<1 %
40	repositorio.uam.es Fuente de Internet	<1 %

41	repositorio.uns.edu.pe Fuente de Internet	<1 %
42	www.themisdata.net Fuente de Internet	<1 %
43	ri.ues.edu.sv Fuente de Internet	<1 %
44	repositorio.upagu.edu.pe Fuente de Internet	<1 %
45	www.repositorio.upla.edu.pe Fuente de Internet	<1 %
46	www.dykinson.com Fuente de Internet	<1 %
47	blog.pucp.edu.pe Fuente de Internet	<1 %
48	datospdf.com Fuente de Internet	<1 %
49	Submitted to Universidad Nacional del Centro del Peru Trabajo del estudiante	<1 %
50	revistas.unc.edu.ar Fuente de Internet	<1 %
51	www.slideshare.net Fuente de Internet	<1 %
52	Submitted to Aliat Universidades	

	Trabajo del estudiante	<1 %
53	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 37 (2021) (VOLUME IV)", Brill, 2023 Publicación	<1 %
54	tesis.pucp.edu.pe Fuente de Internet	<1 %
55	de.slideshare.net Fuente de Internet	<1 %
56	www.churchofjesuschrist.org Fuente de Internet	<1 %
57	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 14 (1998)", Brill, 2001 Publicación	<1 %
58	Submitted to Universidad Nacional de Colombia Trabajo del estudiante	<1 %
59	repositorio.unu.edu.pe Fuente de Internet	<1 %
60	repository.usta.edu.co Fuente de Internet	<1 %
61	dspace.unl.edu.ec Fuente de Internet	<1 %

62	eur-lex.europa.eu Fuente de Internet	<1 %
63	repositorio.pucp.edu.pe Fuente de Internet	<1 %
64	www.perezmora.com Fuente de Internet	<1 %

Excluir citas	Apagado	Excluir coincidencias	< 16 words
Excluir bibliografía	Activo		

DEDICATORIA

A mis padres, María y David, personas llenas de fortalezas, valores, virtudes y amor incondicional, quienes con sacrificio lograron educar a mis hermanas y a mí.

A mis hermanas, Vivian, Leydi y Dayana, y desde el cielo a mi mamita Toribia y a mi abuelita Felicia.

AGRADECIMIENTOS

A Ever Bello Merlo, maestro y asesor, por compartir sus conocimientos y brindar su guía invaluable en el ámbito académico.

A Henry, gran amigo y compañero, con quien disfruté de gratas conversaciones tanto personales como académicas.

RESUMEN

La presente investigación tuvo como objetivo evaluar y analizar el requisito procesal de una pena superior a cuatro años del delito investigado por el Ministerio Público para autorizar judicialmente la intervención o levantamiento del secreto de las comunicaciones, según lo dispuesto en el artículo 230.1 del Código Procesal Penal, y cómo esta limitación afecta la investigación fiscal frente al delito de fraude informático. Asimismo, se analizó el contraste entre el grado de lesividad que causa la medida restrictiva al derecho fundamental en sus niveles de aplicación -información histórica, geolocalización e interceptación de las comunicaciones en tiempo real- y la necesidad de la medida para los intereses de la investigación. Para llevar a cabo esta investigación, se empleó un enfoque cualitativo mediante métodos dogmáticos y sociológicos funcionales, desarrollados con profundidad descriptivo-explicativa. Se utilizaron entrevistas dirigidas a jueces y fiscales como instrumento de recolección de datos para obtener información sobre los criterios que emplean para requerir y autorizar respectivamente el levantamiento del secreto de las comunicaciones. Uno de los principales resultados obtenidos en la investigación fue la limitación que impone el requisito de una pena superior a los cuatro años en la investigación fiscal respecto a los delitos de fraude informático, lo cual deja en impunidad a los posibles autores y partícipes del delito al no poder identificarlos. Esto llevó a la conclusión principal de la necesidad de actualizar el artículo 230 del CPP.

Palabras clave: secreto de las comunicaciones, información histórica, geolocalización, interceptación de las comunicaciones, test de proporcionalidad, fraude informático, medida restrictiva de derechos.

ABSTRACT

The aim of this research was to evaluate and analyze the procedural requirement of a penalty exceeding four years for the crime investigated by the Public Ministry to judicially authorize the intervention or lifting of communications secrecy, as stipulated in article 230.1 of the Criminal Procedure Code, and how this limitation impacts fiscal investigation into computer fraud. Additionally, the study examined the contrast between the degree of harm caused by the restrictive measure to fundamental rights in its application levels—historical information, geolocation, and real-time communication interception—and the necessity of the measure for investigative interests. To conduct this research, a qualitative approach was employed using functional dogmatic and sociological methods, developed with descriptive-explanatory depth. Questionnaires were used as data collection instruments distributed to judges and prosecutors to gather information on the criteria they use to request and authorize the lifting of communications secrecy. One of the main findings of the research was the limitation imposed by the requirement of a penalty exceeding four years in fiscal investigations of computer fraud, which leaves potential perpetrators of the crime unidentified and leads to impunity. This underscores the primary conclusion of the need to update article 230 of the Criminal Procedure Code.

Keywords: communications secrecy, historical information, geolocation, communication interception, proportionality test, computer fraud, restrictive measure of rights.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

ABREVIATURAS

Cas.	Casación.
Corte IDH	Corte Interamericana de Derechos Humanos.
CADH	Convención Americana de Derechos Humanos.
CPP	Código Procesal Penal.
C del PP	Código de Procedimientos Penales
CP	Constitución Política del Perú.
CSJR	Corte Suprema de Justicia de la República.
CSJJU	Corte Superior de Justicia de Junín.
DUDH	Declaración Universal de Derechos Humanos
JIP	Juzgado o juzgados de investigación preparatoria.
PNP	Policía Nacional del Perú
TC	Tribunal Constitucional del Perú.
TEDH	Tribunal Europeo de Derechos Humanos.

INTRODUCCIÓN

Uno de los temas menos explorados en la doctrina procesal es el levantamiento del secreto de las comunicaciones como medida restrictiva de derechos; son pocos quienes se atreven a investigar este tema, aún más cuando existen dificultades al contrastar la teoría con la realidad, debido al difícil acceso a expedientes judiciales que tratan este tema por la reserva de información que conlleva. Sin embargo, esto no me desalentó para desarrollar la presente tesis.

Esta investigación se centró en la intervención de las comunicaciones en el delito de fraude informático, dando énfasis al requisito procesal de la *suma pena* para autorizar judicialmente esta medida, particularmente cuando el delito investigado tiene una pena inferior a cuatro años, considerando que el delito de fraude informático está sancionado con una pena no menor a tres ni mayor a ocho años.

Este tema condujo a criterios diferenciados y a una gran discusión al determinar la pena para cumplir con este requisito; los criterios diferenciados incluyeron la interpretación de la determinación de la pena bajo el sistema de tercios y el criterio de la pena ubicada en el extremo mínimo del delito investigado.

Otro de los puntos importantes de la investigación fueron los grados de lesividad de los tipos de intervención de las comunicaciones y que los resultados sean en mayor medida satisfactorios para el fin buscado, siendo este punto el que recuerda la frase de la serie animada Fullmetal Alchemist, “Para obtener algo, otra cosa de igual valor debe sacrificarse” (Sori, 2003); esto alude al sacrificio de un derecho fundamental para obtener elementos de convicción útiles que posteriormente serán utilizados como prueba en la etapa de juzgamiento.

Asimismo, durante la experiencia como secigrista en la Corte Superior de Justicia de Junín (CSJJU), se evidenció este problema e inspirado principalmente en la intervención de las comunicaciones y la necesidad en la investigación del delito de fraude informático por la dificultad de identificar a los autores y partícipes del delito, consideraba la posibilidad de distinguir los niveles de aplicación de la intervención de las comunicaciones -información histórica, geolocalización e interceptación de llamadas en tiempo real-, con el grado de lesividad que cada uno de estos pueda causar, en aplicación del test de proporcionalidad.

El objetivo principal fue examinar el requisito procesal de *suma pena* para la autorización judicial del levantamiento del secreto de las comunicaciones que limita la investigación en el delito de fraude informático (artículo 230.1 del CPP). Para lograr cumplir con los objetivos de la presente investigación se desarrollaron cuatro capítulos:

En el primer capítulo se plantea la investigación explicando el tema, formulando el problema general y los problemas específicos, así como los objetivos de la investigación; además, se desarrolla la justificación e identificación de sus categorías de análisis como aproximación al estudio.

El segundo capítulo aborda el estado del arte, desglosando aspectos internacionales y nacionales para luego presentar el marco teórico, donde se desarrollan los aspectos conceptuales más importantes para la investigación, junto con algunas críticas y reflexiones sobre el levantamiento del secreto de las comunicaciones y el delito de fraude informático en la regulación peruana.

En el tercer capítulo se detalla el diseño metodológico, utilizando un enfoque cualitativo mediante los métodos dogmático y sociológico funcional, con una profundidad

descriptivo-explicativa; además, se especifica que la técnica utilizada para recoger información fue la entrevista a jueces y fiscales competentes para conocer sobre el levantamiento del secreto de las comunicaciones.

En el cuarto capítulo se procesaron y analizaron los resultados obtenidos de las entrevistas, encontrándose criterios diferentes respecto a la interpretación del requisito procesal de la *suma pena*, principalmente entre los fiscales y jueces entrevistados.

Finalmente, se llegó a tres conclusiones en función de los objetivos y se establecieron recomendaciones orientadas a mitigar el impacto del requisito de la *suma pena* para la intervención de las comunicaciones en el delito de fraude informático.

CAPÍTULO I: Planteamiento de estudio

1.1 Formulación del problema de investigación

Los delitos informáticos han experimentado un aumento significativo, especialmente durante la pandemia por la COVID-19, debido al crecimiento del comercio electrónico a nivel nacional. Según estadísticas del Ministerio Público, los delitos informáticos contra el patrimonio aumentaron en un 117.1 % entre 2020 y 2021, con 11,760 denuncias recibidas (Ministerio de Justicia y Derechos Humanos, 2022).

El artículo 8 de la Ley 30096 (Ley de Delitos Informáticos) establece el delito de fraude informático, que conlleva una pena de tres a ocho años en su tipo base y de cinco a diez años como agravante cuando afecta al patrimonio estatal destinado a fines sociales o asistenciales. Para configurar este delito, es esencial el uso de sistemas informáticos con el propósito de obtener beneficios económicos ilícitos; por lo tanto, la investigación en estos casos requiere el uso de técnicas especiales de investigación.

En este contexto, la intervención en las comunicaciones está regulada por el artículo 230.1 del Código Procesal Penal (CPP), que establece como requisitos para autorizarla: (a) disponer de suficientes elementos de convicción; (b) que la pena del delito imputado sea superior a los cuatro años; y (c) que la intervención sea absolutamente necesaria.

Sin embargo, el delito de fraude informático en su tipo base implica una pena mínima de tres años, lo que no cumple con el requisito de *suma pena* establecido en el CPP, el cual exige una pena mínima de cuatro años. Debido a esta discrepancia, los requerimientos fiscales en estos delitos son declarados improcedentes por los jueces de investigación preparatoria.

Esta situación presenta un grave problema, ya que los delitos informáticos, al ser no convencionales y requerir atención especializada, a menudo demandan medidas de investigación específicas como la intervención en las comunicaciones para identificar a los autores y establecer responsabilidad penal. La falta de autorización judicial debido al incumplimiento del requisito de *suma pena* puede llevar al estancamiento de las investigaciones fiscales, e incluso al archivo o sobreseimiento de los casos, dejando a los delincuentes impunes.

Es evidente que el requisito de *suma pena* plantea un desafío significativo en la investigación del delito de fraude informático, potencialmente contribuyendo a la impunidad al obstaculizar el uso de una medida crucial para esclarecer estos delitos.

La Ley 27697 establece un catálogo de 16 delitos, incluidos los delitos informáticos, en los que se puede aplicar la intervención en las comunicaciones de forma excepcional, sin necesidad de cumplir requisitos procesales. Sin embargo, esto conlleva el riesgo de un uso abusivo de esta medida excepcional en la investigación preparatoria por parte del representante del Ministerio Público y operadores de justicia del Poder Judicial, dado que esta medida, aunque es una herramienta de investigación especial, sigue siendo excepcional, ya que el derecho al secreto de las comunicaciones es la regla general.

Además, es importante destacar que existen dos normas con rango de ley que inciden en este contexto. La primera norma limita la investigación fiscal y la segunda otorga total libertad al fiscal y a los operadores de justicia al momento de solicitar y admitir estas medidas, lo cual podría resultar en prácticas abusivas y arbitrarias.

Este problema se hizo evidente en 2022, durante las labores del autor como secigrista en la CSJJU, al observar la improcedencia de los requerimientos de levantamiento del secreto de las comunicaciones en casos de delitos informáticos, especialmente fraude informático, debido a la falta de cumplimiento del requisito de *suma pena* establecido por el CPP.

Por lo tanto, esta tesis analiza a través de entrevistas los criterios utilizados por los fiscales para solicitar el levantamiento del secreto de las comunicaciones y las decisiones judiciales al respecto, con el objetivo de determinar la necesidad de esta medida en las etapas preliminares y formales de la investigación de delitos de fraude informático.

El propósito de esta investigación es establecer criterios racionales y equilibrados para el uso del levantamiento del secreto de las comunicaciones como una medida de investigación especial y excepcional en delitos informáticos. Estos criterios podrían ser utilizados para reformar el requisito de *suma pena* en relación con esta medida restrictiva, considerando que el CPP contempla tres tipos de intervenciones: (a) información histórica; (b) geolocalización de teléfonos móviles; y (c) intervención en las comunicaciones, cada una con un nivel diferente de afectación a los derechos, según la intensidad de la medida.

En resumen, el levantamiento del secreto de las comunicaciones en su forma histórica se considera menos intrusivo y, por lo tanto, menos lesivo para la privacidad, siendo la medida más adecuada para identificar a los presuntos autores de delitos de fraude informático al proporcionar información general sobre los titulares de las líneas telefónicas involucradas en estos actos ilícitos. El grado de lesividad se analiza a través del test de proporcionalidad, evaluando la idoneidad, necesidad y proporcionalidad estricta de la medida para verificar su necesidad en la investigación.

1.1.1 Problema general

¿Cómo afecta la exigencia del requisito de *suma pena*, establecido en el numeral 1 del artículo 230 del Código Procesal Penal, para la autorización judicial del levantamiento del secreto de las comunicaciones en su forma de información histórica, en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo durante el periodo 2021 y 2022?

1.1.2 Problemas específicos

- ¿En qué medida el requisito de *suma pena* restringe la procedibilidad de los requerimientos fiscales de levantamiento de secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo durante el periodo 2021 y 2022?
- ¿Cuál es el grado de lesividad de la medida restrictiva de derechos de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo durante el periodo 2021 y 2022?

1.2 Objetivo de la investigación

1.2.1 Objetivo general

Examinar cómo la exigencia del requisito de *suma pena* establecido en el numeral 1 del artículo 230 del Código Procesal Penal para la autorización judicial del levantamiento del secreto de las comunicaciones en su forma de información histórica afecta la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo durante el periodo 2021 y 2022.

1.2.2 Objetivos específicos

- Determinar en qué medida el requisito de *suma pena* restringe la procedibilidad de los requerimientos fiscales de levantamiento de secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo durante el periodo 2021 y 2022.
- Evaluar el grado de afectación de los derechos por la medida restrictiva de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo durante el periodo 2021 y 2022.

1.3 Justificación

El estudio de la presente tesis es fundamental debido a que ofrece una propuesta para mejorar el tratamiento del levantamiento del secreto de las comunicaciones en los delitos informáticos, específicamente en el delito de fraude informático. En este contexto, es relevante considerar dos dispositivos legales que regulan esta cuestión: el Código Procesal Penal (CPP) y la Ley 27697. El CPP, en sus artículos 230 y 231, establece los siguientes presupuestos procesales: (a) contar con suficientes elementos de convicción; (b) que la pena del delito investigado sea superior a cuatro años; y (c) que la intervención sea absolutamente necesaria. Por otro lado, la Ley 27697 permite el levantamiento excepcional del secreto de las comunicaciones para un catálogo de dieciséis delitos, incluidos los delitos informáticos.

Sin embargo, en el caso del delito de fraude informático, que tiene una pena de tres a ocho años en su tipo base, no se cumple el requisito de *suma pena* establecido en el CPP,

lo que limita la investigación fiscal y dificulta la identificación de los autores, coautores y/o partícipes del delito, dejándolos en impunidad. Por otro lado, la Ley 27697 permite el levantamiento del secreto de las comunicaciones de manera excepcional, sin requerir los requisitos procesales establecidos, lo que conlleva el riesgo de un uso abusivo y arbitrario de esta medida restrictiva de derechos, a pesar de ser un derecho fundamental reconocido por la Constitución Política (CP) en su artículo 2.10, siendo su levantamiento la excepción.

Por lo tanto, se hace evidente la necesidad de una regulación eficiente respecto al levantamiento del secreto de las comunicaciones. Tanto el CPP como la Ley 27697, en principio, no diferencian los niveles de estos actos especiales de investigación, como la información histórica, la geolocalización de teléfonos móviles y la interceptación de las comunicaciones, a pesar de que estos tienen finalidades diferentes en la investigación y un grado variable de lesividad. La falta de distinción normativa entre estos actos genera el problema mencionado anteriormente.

En este sentido, es crucial proponer una regulación doctrinaria y legislativa que aborde este problema, llegando a un consenso equilibrado donde la norma no limite excesivamente la investigación fiscal y establezca parámetros para evitar el posible uso abusivo de esta medida. Se debe considerar el grado de lesividad de las técnicas especiales de investigación del levantamiento del secreto de las comunicaciones, según su intrusión en el derecho fundamental, diferenciando entre información histórica, geolocalización e interceptación, y estableciendo parámetros de acuerdo con su impacto en dicho derecho.

Para lograr este objetivo, nuestro análisis se centrará en estudiar los criterios de jueces y fiscales competentes para resolver el levantamiento del secreto de las comunicaciones en casos de delitos de fraude informático con penas mínimas inferiores a

cuatro años (tipo base). Esto nos permitirá proponer recomendaciones y criterios más claros que faciliten una adecuada aplicación de estas medidas en el ámbito investigativo.

1.4 Categorías de análisis

Para Strauss y Corbin (2001), las categorías de análisis son el conjunto de procesos de organización de datos según sus propiedades y dimensiones, con el fin de dilucidar las categorías a analizar en la investigación mediante un proceso descriptivo. Este proceso implica operacionalizar los conceptos relevantes que serán útiles en el desarrollo de la investigación, transformándolos en categorías que deben ser analizadas durante el proceso de investigación.

En este contexto, Tamayo y Tamayo (citados en Ramos, 2018) proponen sobre la operacionalización: (a) determinar los conceptos que se desean operacionalizar; (b) dividir los conceptos en dimensiones manejables; y, (c) subdividir las dimensiones en elementos operacionales que puedan ser medidos. Es importante destacar que esta propuesta, aunque se refiere a la operacionalización de variables, se adapta perfectamente al tipo de investigación que se pretende realizar, pudiendo incluso denominarse como operacionalización de categorías.

Para llevar a cabo la operacionalización de nuestras categorías de análisis, determinamos que los conceptos a operacionalizar son el (a) levantamiento del secreto de las comunicaciones; y, (b) el delito de fraude informático, por lo que destacamos lo siguiente:

Tabla 1

Operacionalización de conceptos según categorías

Levantamiento del secreto de las comunicaciones	Delito de fraude informático
1. Derecho fundamental	1. Delitos informáticos
2. Medida restrictiva de derechos	2. Fraude informático
3. Requisitos de procedibilidad	3. Elementos estructurales del delito
4. Test de proporcionalidad	4. Modalidades de fraude informático
5. Finalidad	
6. Tipos de información obtenidas	

Nota: Elaboración propia**.** En esta tabla se dividen los conceptos en categorías.

Tabla 2

Elementos Operacionales

Levantamiento del secreto de las comunicaciones	Delito de fraude informático
1. El secreto de las comunicaciones como derecho fundamental.	1. El fraude informático como delito informático.
2. Medida restrictiva de derechos de levantamiento del secreto de las comunicaciones.	2. Naturaleza y complejidad del delito de fraude informático.
3. Requisitos de procedibilidad para levantar el secreto de las comunicaciones.	3. Elementos del delito de fraude informático.
	4. Modalidades en las que se configuran el delito de fraude informático.

4. Aplicación del test de proporcionalidad en el levantamiento del secreto de las comunicaciones.	
5. Finalidad del levantamiento del secreto de las comunicaciones.	
6. Tipos de información obtenidas con el levantamiento del secreto de las comunicaciones.	

Nota: Elaboración propia. En esta tabla se muestra cómo se subdividen determinan los conceptos a operacionalizar

CAPÍTULO II: Marco teórico

2.1 Antecedentes

En este apartado es fundamental precisar su finalidad, que consiste en desarrollar el estado del conocimiento sobre el levantamiento del secreto de las comunicaciones y sus requisitos procesales, centrándose especialmente en el requisito de *suma pena* y su aplicación en el delito de fraude informático. Es importante señalar que no se han encontrado estudios específicos sobre el levantamiento del secreto de las comunicaciones en relación con el delito de fraude informático. Sin embargo, existen investigaciones generales que abordan aspectos relacionados, aunque no de manera integral. Por lo tanto, se integró, analizó y sistematizó información pertinente sobre este tema para llenar este vacío en la literatura especializada.

2.1.1 Antecedentes internacionales

España. En la legislación española, no se enfrenta el problema de la falta de tratamiento en los distintos tipos de intervención de las comunicaciones, ya que la Ley de Enjuiciamiento Penal Español diferencia entre la intervención en niveles históricos, de geolocalización e interceptación en tiempo real. Estas medidas se encuentran detalladas en su capítulo IV, el cual establece que dichas acciones están sujetas a los principios de idoneidad, necesidad, especialidad, excepcionalidad y proporcionalidad.

Estos principios, que rigen como reglas procesales generales para todos los niveles de intervención, están sujetos a la discrecionalidad del juez para autorizar la medida. Sin embargo, para autorizar la interceptación de las comunicaciones en tiempo real, se establecen requisitos adicionales, a saber: (a) comisión de delitos dolosos con una pena

mínima de tres años; (b) comisión de delitos por un grupo u organización criminal; (c) delitos de terrorismo; y (d) delitos informáticos.

En este contexto, la legislación española no impone limitaciones procesales equivalentes al requisito de *suma pena*. Por el contrario, los límites se establecen a través de principios que guían la discrecionalidad del juez. Es por ello que se enfatiza la importancia de aplicar el test de proporcionalidad. En este sentido, Marco Urgell (2010), en su tesis doctoral, ha concluido que la autorización judicial de las intervenciones telefónicas debe prestar especial atención a: (a) una resolución debidamente motivada; (b) el principio de proporcionalidad; y (c) el control judicial.

Por otro lado, Denise (2021), en su trabajo de fin de grado, concluyó que para autorizar las intervenciones telefónicas deben aplicarse los principios de idoneidad, especialidad, necesidad y proporcionalidad, relacionados con indicios objetivos e intervención en un delito concreto. Incluso en el nivel más intrusivo de intervención de las comunicaciones, como la interceptación, se reconoce que en ciertos delitos esta medida puede ser aplicable, como en el caso de los delitos informáticos, debido a la necesidad en la investigación.

En resumen, la doctrina española no enfrenta dificultades procesales al dictar medidas restrictivas de intervención de las comunicaciones. Sin embargo, existe una preocupación por el uso abusivo de dichas medidas, enfatizando siempre que estas deben estar sujetas a principios rectores que dirijan la discrecionalidad del juez al momento de autorizarlas.

Argentina. La legislación argentina presenta imprecisiones, ya que el Código Procesal Penal Argentino solo regula la interceptación de las comunicaciones sin establecer

requisitos procesales específicos, dejando al juez la tarea de controlar la razonabilidad y legalidad de la medida.

Además, el artículo 7 de la Ley 25760 (normativa argentina), que modificó el artículo 236 del CPP de la Nación, establece que en casos de peligro de demora, el fiscal puede autorizar la intervención mediante una resolución fundamentada y comunicarla de inmediato al juez, quien luego decidirá si la convalida o no.

En este contexto, Salcedo (2012) concluye en su investigación que la autorización para la intervención de las comunicaciones en una investigación penal debe estar sustentada en los principios de proporcionalidad y necesidad. Por su parte, Carbone (2005) se centra en la incorporación de pruebas en el proceso y su legalidad, señalando que la orden judicial es el único requisito constitucional para dictar esta medida.

El problema en la legislación argentina no radica en las limitaciones para autorizar la intervención de las comunicaciones, ya que esta es mucho más flexible y queda a discreción del juez. Esto se destaca especialmente cuando el fiscal está facultado para intervenir las comunicaciones en casos de necesidad e inmediatez, para luego someter la información obtenida al juez competente para su validación judicial.

Sin embargo, queda expuesto que en estos casos puede haber abuso e incluso arbitrariedad por parte del fiscal. Aunque el juez puede subsanar esta situación al convalidar la información obtenida, se habría producido una violación ilegal del derecho al secreto de las comunicaciones.

Colombia. La legislación colombiana aborda de manera general el tratamiento del secreto de las comunicaciones. En el artículo 235 del Código de Procedimiento Penal colombiano, se establece la facultad del fiscal para ordenar la interceptación de

comunicaciones con el propósito de buscar pruebas, evidencia física o ubicar a investigados. Las entidades de telefonía están obligadas a cumplir con la orden del fiscal, quien debe mantener en reserva los datos obtenidos y no puede interceptar las comunicaciones con el abogado defensor. Además, se establece un plazo máximo de tres meses prorrogable.

Los juristas colombianos expresan preocupación debido a que la norma es muy genérica y otorga facultades al fiscal sin control judicial, lo que deja vacíos en la legislación que podrían conducir a márgenes de discrecionalidad inaceptables en la interpretación de la norma y afectar arbitrariamente el derecho al secreto de las comunicaciones (Guerrero Peralta, 2007).

Esta norma no impone restricciones a las medidas adoptadas contra los derechos de los sujetos afectados por la interceptación, lo que implica que el fiscal podría autorizar la medida de manera indiscriminada. No se exigen requisitos procesales ni motivos fundados mediante elementos de convicción, lo que permite al fiscal actuar de manera intuitiva al ordenar la captación de comunicaciones (Farfán, 2007).

2.1.2 Antecedentes nacionales

En el ámbito nacional, Lunarejo y Rodríguez (2021) abordaron en su tesis de pregrado el levantamiento del secreto de las comunicaciones en los delitos informáticos, concluyendo que los delitos informáticos deben considerarse como supuestos especiales para la intervención de las comunicaciones. Sin embargo, es importante señalar que esta tesis, realizada en 2021, no tomó en cuenta la Ley 27697 y sus modificaciones posteriores, las cuales incorporaron la facultad de intervenir las comunicaciones en los delitos informáticos.

Por otro lado, Coronado y Segura (2018), en su tesis de pregrado, propusieron la modificación del artículo 230 mediante la adición del numeral 7, otorgando al fiscal la facultad de realizar la intervención de las comunicaciones a nivel histórico sin autorización judicial, siendo el juez quien posteriormente confirmaría judicialmente la información obtenida. Esta propuesta plantea que esta facultad sería concedida al fiscal cuando el delito investigado tenga una pena superior a los cuatro años.

Es importante considerar que, si bien esta facultad facilitaría la labor de investigación por parte del fiscal, también podría poner en peligro el derecho fundamental al secreto e inviolabilidad de las comunicaciones. Existe el riesgo de un posible uso abusivo de esta facultad, ya que la evaluación del juez de garantías se realizaría después de que el derecho fundamental haya sido restringido o incluso vulnerado. En consecuencia, si el juez no otorga la confirmación judicial, se habría violado el derecho fundamental. No debemos comprometer derechos fundamentales para facilitar la labor de investigación.

2.2 Aspectos teóricos

2.2.1 Secreto e inviolabilidad de las comunicaciones

2.2.1.1 Derecho a la privacidad e intimidad personal. El concepto de privacidad se refiere a la facultad de prevenir la difusión de datos de la vida privada que una persona no desea que sean divulgados. Consiste en evitar ser objeto de intromisiones arbitrarias o ilegales en la vida privada, familiar, y proteger la honra y reputación. Por otro lado, la intimidad personal implica disfrutar de un ambiente reservado y propio para desarrollar libremente una vida personal y familiar plena, excluyendo y evitando intromisiones y conocimiento por parte de terceros.

El avance tecnológico en las comunicaciones (llamadas telefónicas, mensajes de texto, correos electrónicos, redes sociales como Facebook, WhatsApp, Instagram, entre otros), utilizados mediante dispositivos electrónicos modernos (celulares, smartphones, computadoras, laptops, tablets, etc.), ha traído muchos beneficios a la humanidad, pero también nos expone a ataques contra nuestra privacidad a través del uso de internet.

El artículo 12 de la Declaración Universal de Derechos Humanos (DUDH) establece que nadie debe ser objeto de ataques a su honra, reputación, ni injerencias en su vida privada; mientras que la Convención Americana sobre Derechos Humanos (CADH), en su artículo 11.2, prescribe la protección de estos derechos.

En este contexto, Noya (2000) diferencia entre el derecho a la vida privada, que es un concepto general que abarca todos los derechos que protegen la reserva de un individuo, incluyendo la protección de la persona, la familia, las comunicaciones privadas y las actividades realizadas en el hogar. Este término se utiliza como sinónimo de intimidad en su sentido más amplio. Por otro lado, el concepto de intimidad se refiere únicamente a las manifestaciones más íntimas y secretas de la vida privada.

El derecho a la intimidad reconoce tres esferas principales: (a) esfera íntima, que incluye el ámbito interno de la persona, como su vida sexual y su mundo mental; (b) esfera personal, que abarca la vida cotidiana de la persona y sus relaciones con amigos y conocidos cercanos; (c) esfera social pública (Monzón, 2015).

En resumen, la vida privada comprende todas aquellas circunstancias que, sin ser íntimas o secretas, merecen el respeto de todos para garantizar la tranquilidad y el desenvolvimiento normal de sus titulares. El respeto de la esfera privada es un derecho que protege a la persona contra la divulgación indebida de sucesos familiares o particulares, sin

importar si son secretos o no, y sin considerar su veracidad. Podemos concluir que ambos derechos están vinculados, ya que el derecho a la privacidad es el género y la intimidad personal es una especie dentro de este género.

2.2.1.2 Derecho al secreto de las comunicaciones. Los seres humanos somos sociables por naturaleza, lo que nos lleva a compartir reflexiones, vivencias y experiencias con otras personas en nuestro entorno social, utilizando para ello la comunicación y, en la actualidad, instrumentos tecnológicos como internet, mensajes de texto, llamadas telefónicas, correos electrónicos, entre otros. A través de estos medios, podemos expresar ideas, tendencias e incluso sentimientos hacia otras personas. Es por ello que los legisladores han tomado conciencia del riesgo para la vida privada que conllevan los avances tecnológicos e informáticos, estableciendo el derecho al secreto de las comunicaciones para proteger contra la intromisión ilegal en las comunicaciones, sus instrumentos y el conocimiento de terceros no autorizados por el emisor.

El derecho al secreto de las comunicaciones establece garantías objetivas que protegen toda comunicación, independientemente de su contenido. Esto significa que no importa si la comunicación contiene aspectos íntimos y privados de la vida de una persona o si se refiere a otros aspectos, incluso intrascendentes (Díaz, 2006). Por su parte, Carbone (2005) sostiene que este derecho fundamental garantiza al interlocutor la confidencialidad no solo del contenido de la comunicación, sino también de los datos externos como el tiempo, la duración y el destino de la llamada, independientemente del medio de transmisión.

Es importante entender que el secreto de las comunicaciones protege no solo el contenido de la comunicación, sino también el instrumento utilizado y las circunstancias

que la rodean. Cada individuo tiene la capacidad de controlar sus propias conversaciones y decidir con quién desea compartirlas. Sin embargo, para que una conversación sea considerada secreta, el medio utilizado debe permitir una comunicación privada. Por ejemplo, las comunicaciones transmitidas por medios dirigidos al público en general, como la radio y la televisión, no están protegidas por el derecho al secreto de las comunicaciones. En cambio, este derecho protege las comunicaciones que permiten la conversación entre dos o más personas de manera privada o cerrada, como las videoconferencias, llamadas telefonicas, etc.

Es importante destacar que quien graba una conversación propia no está infringiendo el derecho al secreto de las comunicaciones, siempre y cuando no revele posteriormente el contenido de manifestaciones íntimas vertidas en esa comunicación. La divulgación de tales manifestaciones sí constituiría una intromisión al derecho a la intimidad.

Feijóo (2021) argumenta que el derecho al secreto de las comunicaciones es autónomo y diferente al derecho a la intimidad. Aunque son derechos independientes, ambos están relacionados en la protección de la vida privada.

En resumen, el derecho al secreto de las comunicaciones está estrechamente vinculado con la privacidad y la intimidad personal. Castillo (2022) señala que este derecho prohíbe que terceros intervengan o conozcan la comunicación que una persona tiene con otras, mientras que la inviolabilidad de las comunicaciones protege toda conversación, independientemente de su contenido, respecto a cualquier persona, ya sea tercero o no. El derecho al secreto de las comunicaciones protege el contenido de la comunicación en sí mismo.

2.2.1.3 El secreto de las comunicaciones como derecho fundamental. Los derechos fundamentales son derechos innatos y no adquiridos, reconocidos por el Estado con el fin de asegurar y proteger la dignidad humana y el desarrollo personal, independientemente del nivel económico o social de las personas. Estos derechos humanos, reconocidos a nivel nacional por nuestra Constitución Política, comparten el mismo contenido que los derechos humanos adoptados a nivel supranacional o internacional (Noya, 2000).

El TC ha establecido que los derechos fundamentales tienen una dimensión objetiva que responde al objeto de protección del derecho, y una dimensión subjetiva que protege al sujeto titular del derecho. Ambas dimensiones componen el derecho fundamental, el cual es protegido por el Estado a través de garantías subjetivas e institucionales para salvaguardar tanto al titular como al objeto del derecho (Exp. N°.01470-2016-PHC/TC).

En un estado de derecho, el aspecto legislativo está vinculado con los derechos humanos mediante la incorporación de estos últimos en la Constitución (Alexy, 2000). Cuando esto sucede, los derechos humanos reconocidos adoptan el nombre de derechos fundamentales.

Es importante destacar que los derechos fundamentales no son absolutos, ya que si lo fueran no podrían ser restringidos en ningún sentido, afectando así los intereses estatales y colectivos (Peña, 2011). En el caso del derecho al secreto de las comunicaciones, este puede ser restringido cuando está previsto en la norma y existe un legítimo interés social.

La CIDH considera que el derecho al secreto de las comunicaciones como una extensión del derecho a la vida privada, a pesar de que no esté explícitamente reconocido en la Convención. Esto significa que el derecho está dotado de protección, especialmente

en casos de intervenciones telefónicas que interfieren en la vida privada (Escher et al., 2009).

El fundamento del derecho al secreto de las comunicaciones radica en la confidencialidad de las comunicaciones, garantizando el secreto del contenido y el proceso de las mismas frente a la intermediación de terceros (Carbone, 2005). Las escuchas no autorizadas judicialmente suponen una vulneración de este derecho.

Este derecho consagra la libertad de comunicación y establece protección contra el conocimiento ilegal de las comunicaciones ajenas mediante interceptación, captación o conocimiento ilícito de las comunicaciones. Sin embargo, existen excepciones establecidas en nuestra Constitución Política.

Nuestra Constitución Política reconoce el derecho fundamental al secreto de la comunicación y los instrumentos que lo permiten, aunque también establece excepciones. Las comunicaciones y sus instrumentos solo pueden ser incautados, abiertos, intervenidos o interceptados mediante mandato motivado por el juez y respetando las garantías establecidas por ley.

Asimismo, Castillo (2022) señala que el artículo 2.10 de la Constitución Política regula el derecho fundamental al secreto de las comunicaciones, que incluye el derecho fundamental, la inviolabilidad de la comunicación, la inviolabilidad de los instrumentos de comunicación y la inviolabilidad de documentos privados.

Es importante destacar que un derecho fundamental debe considerarse verdaderamente eficaz solo si no solo está establecido en la norma, sino que también es garantizado de manera efectiva en caso de su violación (Romboli, 2017). Por lo tanto, todo derecho fundamental debe recibir un tratamiento especial, especialmente cuando existen

excepciones, garantizando que no se lesione más allá de lo permitido y teniendo especial rigurosidad al determinar la imperiosa necesidad de dictar medidas en su contra.

2.2.1.4 Medida restrictiva al derecho del secreto de las comunicaciones. La intervención telefónica es un acto especial de investigación que restringe el derecho al secreto de las comunicaciones y, dada su naturaleza, es requerida únicamente por el fiscal durante la etapa de investigación preparatoria. Esta intervención solo puede ser autorizada mediante una resolución motivada por el juez de garantías, permitiendo la interceptación del contenido de las comunicaciones y/o sus instrumentos. La finalidad de esta medida es obtener datos que ayuden a determinar la responsabilidad del delito, individualizar a los investigados, establecer las circunstancias del delito y obtener material incriminatorio para utilizarlo en el juicio oral.

Por otro lado, Blancas (2012) afirma que la intervención telefónica se lleva a cabo durante la investigación preparatoria en relación con delitos especialmente graves. El juez de garantías toma la decisión, mediante un auto debidamente fundamentado, de permitir que la autoridad policial o la fiscalía registre llamadas y/o grabe conversaciones telefónicas del sospechoso o de personas relacionadas con el delito investigado. Esta acción se realiza durante el tiempo necesario para identificar al autor y determinar la responsabilidad penal mediante medios probatorios.

El artículo 2.10 de nuestra CP establece una excepción a este derecho fundamental, indicando que las comunicaciones solo pueden ser intervenidas por mandato motivado del juez, quien debe tener en cuenta las garantías previstas por ley. Por su parte, el artículo 230.1 del CPP desarrolla los requisitos de procedibilidad que debe cumplir el requerimiento del fiscal para el análisis de fondo por parte del juez de garantías. Estos requisitos incluyen:

(a) disponer de suficientes elementos de convicción; (b) que la pena prevista sea mayor a cuatro años; y (c) que la intervención sea estrictamente necesaria para continuar con la investigación. Si alguno de estos requisitos no se cumple, el juez de garantías rechaza el requerimiento fiscal sin analizar el fondo del asunto, incluso si la medida es estrictamente necesaria y cuenta con suficientes elementos de convicción, cuando la *suma pena* prevista para el delito investigado es menor a cuatro años.

Sin embargo, la Ley 27697 establece un catálogo de dieciséis delitos en los que el levantamiento del secreto de las comunicaciones puede realizarse de manera excepcional, sin limitaciones procesales previas, para los delitos contemplados en dicha ley, incluyendo los delitos informáticos.

Ambas normativas ocupan un espacio definido, siendo la primera con requisitos procesales que limitan la investigación del delito y, como consecuencia, pueden resultar en el archivo de la carpeta fiscal o el sobreseimiento del expediente judicial, dejando impunes a los autores, coautores y partícipes del delito. En cambio, la segunda normativa permite el levantamiento excepcional del secreto de las comunicaciones sin requisitos previos, lo que podría conducir a un posible abuso de esta medida.

Castillo (2022) señala que toda afectación a un derecho fundamental constituye un acto limitado, circunscrito y vinculado a cada caso en concreto. La excepcionalidad y lesividad de esta medida exigen una eficacia limitada en sus efectos y una vinculación a los hechos del proceso o investigación que la genera.

Es arbitrario pretender utilizar una medida tan restrictiva y que afecta intensamente un derecho fundamental para investigar y acreditar cualquier delito o hecho ilícito, y solo

se justificaría si se utiliza para obtener información probatoria de delitos de especial dificultad en la investigación.

Es importante mencionar que el Tribunal Europeo de Derechos Humanos (TEDH) ha precisado que existen intervenciones de menor injerencia, como la entrega de información histórica por parte de las compañías telefónicas en casos penales, que son de menor intensidad que las escuchas telefónicas (Caso Malone contra el Reino Unido, 1984).

Asimismo, es fundamental destacar que, aunque la medida restrictiva del derecho al secreto de las comunicaciones debe ser autorizada y controlada por la autoridad judicial, esta medida resulta insuficiente para prevenir el uso arbitrario de criterios por parte de los magistrados, lo que subraya la necesidad de un sistema jurídico que brinde protección a este derecho (De Langhe, 2009).

2.2.1.5 Protocolo de actuación conjunta de la interceptación de comunicaciones. Los artículos 230 y 231 del CPP desarrollan de manera genérica la intervención de las comunicaciones, al igual que la Ley 27697, la cual otorga facultades al Fiscal para la intervención y control de comunicaciones y documentos privados en casos excepcionales. Además, el protocolo de actuación conjunta de medidas restrictivas de derechos aprobado por el Ministerio Público y el Poder Judicial desarrolla con mayor amplitud el procedimiento de la intervención de las comunicaciones. En este sentido, se han identificado cuatro momentos principales: (a) sede policial, (b) sede fiscal, (c) sede judicial y (d) ejecución.

Sin embargo, es importante señalar que la resolución administrativa mencionada presenta un razonamiento desfasado en cuanto a la aplicación de la norma. Indica que si la investigación está vigente en el distrito judicial, se utilizará únicamente la norma general

del CPP, mientras que en los distritos donde esté vigente el Código de Procedimientos Penales (C. de PP) se aplicará lo dispuesto en la Ley 27697, modificada en el año 2019. Por esta razón, es indispensable actualizar la resolución administrativa N° 134-2014-CE-PJ, ya que, a pesar de sus deficiencias, es la única guía que detalla conceptos y procedimientos para la intervención de las comunicaciones a nivel policial, fiscal y judicial, como:

Informe policial. Los efectivos policiales se encuentran en primera línea en las investigaciones criminales y a menudo se enfrentan a barreras que pueden limitar la investigación. Por lo tanto, es de extrema necesidad llevar a cabo actos especiales de investigación que impliquen restricciones de derechos, como la intervención de las comunicaciones, para evitar que la investigación se estanque ante un delito.

En este contexto, el personal policial a cargo de una investigación criminal que requiera levantar el secreto de las comunicaciones debe presentar un informe al fiscal correspondiente solicitando la autorización para intervenir las comunicaciones. Este informe debe verificar que existan suficientes elementos de convicción e indicios de sospecha inicial simple, así como demostrar la estricta necesidad de la medida.

La resolución administrativa N° 134-2014-CE-PJ establece que el informe policial debe contener al menos los siguientes elementos:

- La necesidad de la medida.
- Indicios o elementos de convicción suficientes que respalden la solicitud.
- Identificación de las personas afectadas (en caso contrario, se deben explicar las razones).

- Datos y/o instrumentos de comunicación que serán objeto de intervención.
- Duración prevista de la medida.
- Indicación de la oficina de apoyo técnico judicial de la PNP como soporte para la ejecución de la medida.

En el informe policial también se puede solicitar información adicional, como la identificación de personas y otros datos, números telefónicos, SIM, IMEI, IMSI, dirección IP, correos electrónicos, entre otros.

Requerimiento fiscal. Una vez presentado el informe policial, el fiscal debe evaluar si el informe policial se encuentra debidamente fundamentado y contenga los datos necesarios, en este caso el fiscal formulara su requerimiento al Juzgados de Investigación Preparatoria (JIP), este requerimiento debe contar mínimamente con los requisitos de procedibilidad descritos en el artículo 230.3 del CPP estos son: (a) cuente con el nombre, dirección, identidad del teléfono -si se conociera-; (b) debe señalar la forma de intervención, alcance y duración; y, (c) se debe indicar el personal policial que se encargara de la diligencia.

Mediante resolución administrativa N° 134-2014-CE-PJ, señala que el requerimiento fiscal debe contener mínimamente: (a) Descripción del hecho delictivo investigado; (b) imputación del delito con una pena superior a los cuatro años; (c). Suficientes elementos de convicción; (d); la necesidad de la medida y su finalidad; (e) identidad del sujeto; (f). Datos de identificación del bien afectado, así como del instrumento de la comunicación; (g) la forma de intervención (información histórica, geolocalización y/o interceptación de las comunicaciones).

Es necesario precisar que el fiscal requiere la intervención de las comunicaciones, sin la necesidad de que la policía emita un informe solicitando la medida, pues el CPP, lo faculta y la ley específica -Ley N º 27697- no lo prohíbe, en este sentido debemos recordar que el fiscal es director de la investigación -artículo 60 del CPP-, mientras que la Policía brinda auxilio al Ministerio Publico en las labores de investigación -artículo 67 del CPP-; es de señalar que la policía también realizan actos de investigación, en la que pueden evidenciar la necesidad de obtener información relevante que coadyuve con el esclarecimiento de los hechos, que únicamente se puede conocer mediante la intervención de las comunicaciones para la interceptación de la misma; a fin de que la investigación no se estanque, en estos casos el fiscal actúa como un primer filtro, para luego requerir la medida ante el juez de Investigación Preparatoria para que dicte la medida.

Resolución judicial. Una vez cumplidos los requisitos procesales exigidos en el artículo 230 del CPP, el juez debe emitir su decisión mediante una resolución debidamente motivada, autorizando o rechazando la solicitud de intervención de las comunicaciones. Esta decisión es comunicada al fiscal, quien junto con el personal policial autorizado se encargará de llevar a cabo la intervención dentro del plazo establecido en la resolución judicial. Las empresas de comunicaciones y telecomunicaciones están obligadas a colaborar con la investigación y a proporcionar la información requerida.

Además, según la resolución administrativa N° 134-2014-CE-PJ, el juez debe examinar el requerimiento fiscal para verificar si cumple con los requisitos necesarios:

- Identidad del requirente (fiscal)
- Descripción detallada del hecho

- Pena no menor de cuatro años (en los distritos judiciales bajo el CPP) o delitos contemplados en el artículo 1 de la Ley 27697 (en distritos bajo el C. de PP)
- Indicios que sustenten la solicitud
- Razones que justifiquen la necesidad, idoneidad y proporcionalidad de la medida, así como su finalidad
- Identidad de la persona afectada
- Datos de identificación del bien o instrumento de comunicación afectado
- Duración prevista de la medida
- Especificación de quién ejecutará la intervención
- Una vez concluida la intervención, se informarán los resultados al juez de garantías para el respectivo control
- El juez decidirá sobre la forma de intervención sin mencionar los detalles técnicos o mecanismos utilizados

2.2.1.6 Críticas al protocolo de actuación conjunta sobre la intervención o grabación de registro de comunicaciones telefónicas o de otras formas de comunicación. En principio, el vigente protocolo de actuación conjunta publicado en 2014 se encuentra desactualizado, siendo el único documento que detalla el procedimiento para medidas restrictivas de derechos en la búsqueda de pruebas, incluyendo el procedimiento de intervención de las comunicaciones.

El protocolo hace referencia a la Ley 27697, la cual ha tenido múltiples modificaciones, siendo la última en el año 2019. Asimismo, establece que esta última es aplicable para los distritos judiciales en los que aún se utiliza el C. de PP, mientras que en los distritos judiciales donde se encuentra vigente el CPP se aplicarán las disposiciones

establecidas en los artículos 230 y 231 del mismo cuerpo normativo. Es importante destacar que el CPP está vigente de manera integral en todos los distritos judiciales del país (UETI-CPP, s.f.). A pesar de la existencia de los juzgados liquidadores que aún utilizan el C. de PP, este protocolo también queda desfasado para la intervención de las comunicaciones, ya que esta medida por su naturaleza solo se utiliza en la etapa de investigación preparatoria.

El juez debe verificar si el delito cumple con los requisitos procesales o si está contemplado como delito grave en la ley 27697. Esta posición sugiere que ambos cuerpos normativos no son contradictorios entre sí; por el contrario, el criterio para aplicar los requisitos procesales del CPP no se aplica cuando el delito investigado está incluido en la lista de delitos previstos en la ley especial (Abad, 2012).

Esto se debe a que la ley especial es una norma que se considera excepcional y se basa en criterios específicos o cualidades de ciertos asuntos. Estas leyes se refieren específicamente a una materia particular. En esencia, surgen debido a la necesidad de regular situaciones fundamentalmente distintas de aquellas que aplican a situaciones comunes o genéricas. Como consecuencia de esta regla, una ley especial tiene prioridad sobre una ley de carácter general (Exp. N.° 018-2003-AI/TC, 2004).

La posición del TC es preferir la aplicación de una ley especial o específica sobre una norma de carácter general. En este contexto, el CPP se considera la norma general, mientras que la norma especial es la Ley 27697, por lo que consideramos que el protocolo de actuación conjunta al menos en el criterio que adopta sobre la aplicación de ambas normativas en los diferentes distritos judiciales del país es erróneo.

Con lo mencionado anteriormente, sostenemos que el protocolo de actuación conjunta se encuentra desactualizado y necesita modificarse, no solo en la interpretación

del uso de la norma general y especial, sino también actualizando el procedimiento conforme a la actualidad.

Es importante señalar que el uso de la norma general limita la investigación realizada por el fiscal con el requisito de una pena superior a los cuatro años, mientras que con la ley especial no se exigen requisitos procesales, otorgando plena libertad al fiscal y al juez para considerar la intervención de las comunicaciones, lo cual podría restringir el derecho al secreto de las comunicaciones de manera innecesaria y posibilitar el uso abusivo e incluso arbitrario de esta medida.

2.2.1.7 Interpretación de las normas que regulan el levantamiento del secreto de las comunicaciones. En relación con este tema, la Corte Suprema de Justicia de la República (CSJR) ha señalado que la teoría general del derecho ha propuesto tres criterios para determinar la norma aplicable en estos casos:

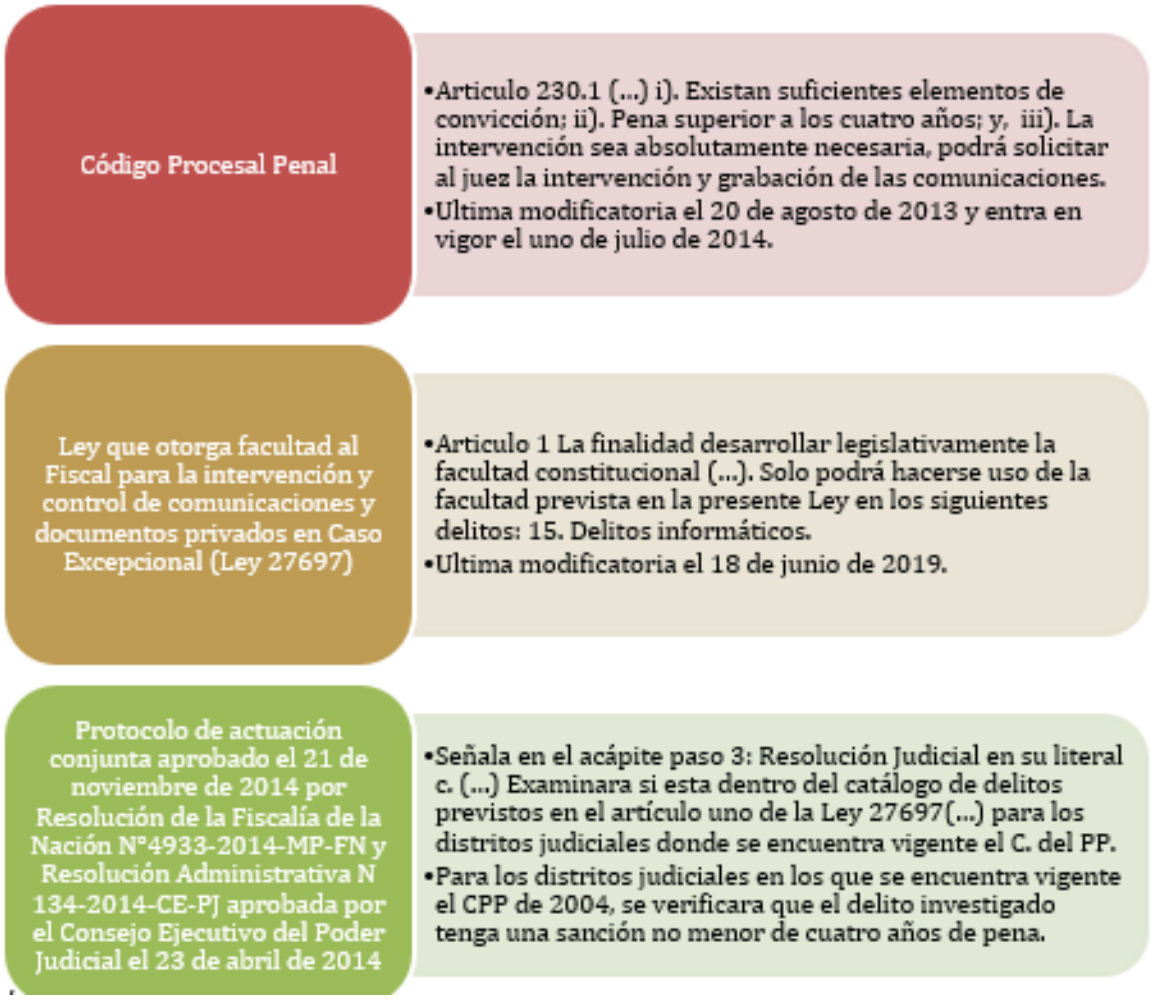
- **Criterio de jerarquía.** Este criterio establece que una norma de rango superior prevalece sobre una norma de rango inferior. Una norma se considera jerárquicamente superior cuando la validez de otra norma depende de ella.
- **Criterio de especialidad.** Este criterio establece que una norma especial tiene prioridad sobre una norma general. Este principio, ampliamente aceptado en el derecho, significa que cuando existen normas específicas que se aplican a una situación particular, esas normas deben prevalecer sobre las normas generales que tratan sobre el mismo tema.
- **Criterio de temporalidad.** Este criterio determina que una norma posterior en el tiempo prevalece sobre una norma anterior. En otras palabras, cuando se promulga

> una nueva norma que modifica o deroga una norma anterior, la norma más reciente es la que debe aplicarse (Casación N° 342 - 2011 Cusco).

Es importante destacar, en relación con el conflicto interpretativo de la norma en referencia a la medida restrictiva del derecho al secreto de las comunicaciones, específicamente en lo que respecta al requisito de que el delito debe ser sancionado con una pena superior a los cuatro años:

Figura 1

Requisitos procesales para autorizar la intervención de las comunicaciones



Nota. Elaboración propia. El grafico describe las diferencias entre los requisitos procesales para levantar el secreto de las comunicaciones en la norma general, especial y la interpretación del protocolo de actuación conjunta.

En este sentido la interpretación de las normas que regulan la intervención de las comunicaciones en nuestra legislación bajo criterios establecidos por la CSJR, debemos señalar lo siguiente:

- **Principio de jerarquía.** El CPP y la Ley 27697 comparten la misma jerarquía, es decir ambos cuerpos normativos tienen la calidad de normas con rango de Ley.

- **Principio de especialidad.** El CPP es la norma general, mientras que la Ley 27697 tiene la calidad de norma especial al desarrollar exclusivamente la intervención de las comunicaciones.
- **Principio de temporalidad.** Mientras que el Protocolo de Actuación Conjunta interpreta que la aplicación del CPP en los distritos judiciales en los que se encuentre vigente, mientras que la Ley 27697 -modificatoria el 18 de junio de 2019- en aquellos donde aún rige el C. de PP, al respecto es importante precisar que en todos los Distrito Judiciales del Perú rige el CPP, siendo el último en integrarlo el distrito judicial de Lima Sur el 15 de junio de 2021 (UETI-CPP, s.f.), entendiéndose que la norma especial habría perdido vigencia, empero el artículo 103 de la CP, que prescribe que una norma solo puede ser derogada por otra Ley.

Razones por las que, al tratarse de normas del mismo nivel jerárquico, primando la especialidad en el Ley 27697, empero bajo el principio de temporalidad la mencionada ley especial habría perdido la naturaleza de su vigencia según el criterio adoptado por el Ministerio Publico y el Poder Judicial, esto es un grave problema en la interpretación normativa al momento de utilizar los cuerpos normativos señalados.

2.2.1.8 Requisitos de procedibilidad para levantar el secreto de las comunicaciones. En la legislación peruana, la intervención de las comunicaciones solo se autoriza cuando la hipótesis fiscal parte de la comisión de un delito con una pena superior a cuatro años. Según Castillo (2022), el CPP adopta un criterio objetivo concreto para los delitos que superan la *suma pena*. En el Perú, la gravedad del delito no se mide por la lesión al bien jurídico protegido, la trascendencia social del hecho, sino por el criterio de la gravedad de la pena.

Carbone (2008) señala que el principio de especialidad de la intervención de las comunicaciones requiere que la resolución judicial que autoriza la medida contenga con claridad:

- El hecho delictivo que se está investigando, delimitado espacial y temporalmente.
- Una pena superior a cuatro años.
- La debida identificación de la persona investigada.
- Datos del titular de la línea intervenida.
- La identificación y el número telefónico intervenido.

Por otro lado, De Langhe (2009) establece que en la legislación argentina, la intervención de las comunicaciones debe cumplir con:

- Pertenecer a un catálogo de delitos.
- Preexistencia de un proceso penal en trámite.
- Motivación suficiente (cierto grado de sospecha y test de proporcionalidad).
- Sujetos afectados.
- Duración de la medida.
- Registro de la intervención.
- Control jurisdiccional.

2.2.1.9 Requisito de la pena para autorizar judicialmente la intervención. Como se mencionó anteriormente, es necesario que el delito investigado tenga una pena superior a cuatro años para justificar la intervención de las comunicaciones, siendo este el punto central de la investigación. En este contexto, se han considerado dos aspectos:

(a) Interpretación de la pena bajo el sistema de tercios para superar el requisito de la *suma pena*. El sistema de tercios divide la pena legal en tres segmentos: tercio inferior, medio y superior. A través de este método, se aplican circunstancias atenuantes y/o agravantes, según lo establecido en el Código Penal en el artículo 45-A, con el fin de determinar en qué segmento se ubica finalmente la pena. Este proceso implica una evaluación técnica y valorativa por parte del juez para precisar la gravedad cuantitativa y cualitativa del delito y, en ocasiones, la ejecución de la pena (Casación N° 723-2018 Junín).

La CSJR ha afirmado que la determinación de la pena implica concretar la sanción penal mediante el uso del sistema de tercios, considerando el injusto y la culpabilidad del hecho, así como el principio de proporcionalidad de la pena (Casación N° 68-2019 Lambayeque).

En conclusión, la determinación de la pena bajo el sistema de tercios es un mecanismo legal diseñado para ser utilizado durante el juicio para establecer una pena específica. Prado (2018) también señala que la determinación judicial de la pena en la legislación peruana se basa en este sistema para la aplicación de una pena concreta durante el juicio.

(b) Interpretación del requisito de una pena superior a cuatro años en el extremo mínimo del delito investigado. Bajo el principio in dubio pro reo, establecido en el artículo 139.11 de la Constitución, se debe interpretar la norma de manera más favorable para el investigado en caso de duda o contradicción. En este contexto, la interpretación más favorable para el investigado es aquella que limite más la intervención de las comunicaciones, dado que afecta un derecho fundamental, ya sea de manera lícita o ilícita. Por lo tanto, es fundamental considerar el extremo mínimo de la pena del delito investigado, ya que una interpretación contraria afectaría este principio.

Además, el principio in dubio pro reo refuerza el argumento de que el sistema de tercios no puede aplicarse en la etapa de investigación preparatoria, ya que está diseñado para ser utilizado en el juicio, una vez que se ha determinado el injusto y la culpabilidad del acusado.

Es necesario tener en cuenta estas razones para comprender la incongruencia en la aplicación del sistema de tercios para superar el requisito de una pena superior a cuatro años en el contexto de la intervención de las comunicaciones, que es un método especial de investigación.

2.2.1.10 Formas de intervención y tipos de información obtenidas con el levantamiento del secreto de las comunicaciones. En el contexto del levantamiento del secreto de las comunicaciones, es relevante destacar que existen hasta cuatro formas de intervención, cada una con un nivel de afectación distinto al derecho al secreto de las comunicaciones, así como con requerimientos específicos para la investigación fiscal.

Información histórica. La obtención de información histórica mediante la intervención de las comunicaciones es una medida no intrusiva en el contenido de las comunicaciones según nuestra legislación. De acuerdo con lo establecido en el protocolo de actuación conjunta, los proveedores de servicios públicos de telecomunicaciones pueden proporcionar la siguiente información histórica:

- Datos de filiación (información general del titular de la línea).
- Registro de datos de comunicaciones: número telefónico, IMSI e IMEI del objetivo e interlocutor, fecha, hora y duración de la comunicación, tipo y dirección de la comunicación; Modem/Router o BTS inicial y final (código, nombre, dirección, latitud, longitud y sector).

- Ubicación desde donde se originó la comunicación y cualquier otro dato de comunicación registrado.
- Datos de localización o geolocalización en tiempo real y/o actual.
- Datos de dispositivos móviles registrados en Modem/Router o BTS, en un rango de fecha y hora determinada, así como su ubicación.

Esta información puede obtenerse cuando se necesita información histórica derivada de la intervención del secreto de las comunicaciones que afecte al instrumento de comunicación o telecomunicación. Por lo tanto, existe la posibilidad de acceder a datos de telecomunicaciones almacenados por las compañías prestadoras de servicios posteriormente al momento de la comunicación (Varona, 2020).

Interceptación de las comunicaciones en tiempo real. La interceptación de las comunicaciones en tiempo real o intervención de las comunicaciones, es la medida restrictiva del derecho al secreto de las comunicaciones más lesiva, pues el impacto de estos actos especiales de investigación recae en el contenido de la comunicación mediante escucha de llamadas telefónicas.

Asimismo, Varona (2020), señala que cuando la interceptación se produce en el momento en que se realiza la comunicación con sistemas utilizados para la ejecución de la interceptación el cual habilita para no solo escuchar y grabar el contenido de las comunicaciones telefónicas, sino también para acceder a determinados datos como son el número de origen y destino de las comunicaciones, así como acceder a la ubicación en el espacio de los intervinientes en la llamada.

En un sentido similar, Blancas (2012) sostiene que, las conversaciones grabadas en formato magnético u otros medios técnicos similares las obtendrá el Fiscal, quien deberá

conservar dicha información con las medidas de seguridad adecuadas y garantizar que terceras personas no accedan a ella, asimismo ordenará la transcripción escrita de las grabaciones, levantando en acta, y conservar las grabaciones. En caso de que haya comunicaciones irrelevantes para el procedimiento, estas se entregaran a las personas afectadas por la medida, y cualquier transcripción de estas serán destruidas por el Ministerio Público.

Geolocalización. La geolocalización es uno de los actos especiales de investigación de un delito, para la cual se requiere de los mismos requisitos procesales establecidos en el CPP, empero en caso de flagrancia delictiva el Decreto Legislativo N° 1182 regula el uso de datos para la identificación, localización y geolocalización de equipos de comunicación, pues esta cuenta con requisitos procesales especiales en la referida ley para tal fin, estos son: (a) flagrante delito; (b) La pena sea superior a los cuatro años; y, (c) el acceso a los datos constituye un medio necesario para la investigación.

En este sentido la referida ley establece como finalidad regular el acceso de la unidad especializada de la PNP a la localización de teléfonos móviles, asimismo es de señalar que para efectos de la geolocalización.

Asimismo, se señala que no es necesario requerir la autorización judicial para dicho fin, pues el procedimiento que se sigue se limita únicamente a la sede policial y fiscal, pues según el Decreto Legislativo N° 1182 el procedimiento comienza cuando (a) el personal policial pone en conocimiento del hecho al fiscal, para que este requiera directamente a la unidad especializada para ejecutar la geolocalización; (b) una vez recibida el requerimiento, se requiere a los concesionarios de comunicaciones y/o entidades públicas relacionadas con estos servicios; (c) los concesionarios de servicios de comunicaciones se

obligan a brindar datos de localización y geolocalización de manera inmediata; y, (d) Con esto la unidad especial de investigación realiza diligencias derivadas de la geolocalización.

Después de analizar este acto especial de investigación, podemos concluir que se trata de actos urgentes e inaplazables, empero esta también es parte de una medida restrictiva de derechos, por lo que requiere de la actuación del fiscal para evitar el abuso de la medida.

Las facultades de geolocalización se vinculan al uso de tecnologías de la información y comunicaciones, lo que implica el acceso a la metadata, lo que implica el acceso a la información sobre la información, siendo este concepto en las telecomunicaciones el vínculo entre el origen y destino de llamadas, mensajes electrónicos y mensajes instantáneos. Pues a pesar de que no se tiene acceso al contenido, se pondrá en posición al contenido de la comunicación, se podrá conocer la posición de una persona y la de todos los que intercambian mensajes con él (Quiñonez y Marlon, 2015).

En este sentido la geolocalización resulta ser una forma de la intervención de las comunicaciones, que no afecta al contenido de la comunicación, pero si a su instrumento, es por ello la necesidad del referido Decreto Legislativo de establecer como obligación de la convalidación judicial.

La crítica viene con el artículo 6 del referido Decreto Legislativo al señalar que la geolocalización o localización se excluye de cualquier intervención de las comunicaciones, cuando afectan al instrumento de la comunicación, recordemos que el secreto de las comunicaciones protege también al instrumento de la comunicación; empero considero acertada el Decreto Legislativo, pues esta tendría la condición de ley especial.

2.2.1.11 Ejecución de la medida del levantamiento del secreto de las comunicaciones. Una vez que el Juez ha emitido la autorización para la medida, es responsabilidad de la policía y la fiscalía llevar a cabo la intervención y grabación de las conversaciones según lo dispuesto. Para ello, las empresas de telecomunicaciones tienen la obligación de facilitar la ejecución dentro del plazo establecido en la resolución judicial.

Durante la ejecución de la medida, que implica la recolección o registro de las comunicaciones, el fiscal recopila toda la información obtenida, la resguarda y descarta lo que no sea relevante para la investigación (Arbulu, 2015).

2.2.1.12 La búsqueda de pruebas con el levantamiento del secreto de las comunicaciones. Desde la perspectiva jurídica procesal, la intervención de las comunicaciones es una técnica de investigación que permite obtener medios de prueba, los cuales no existían antes de la investigación, sino que se forman en el momento de la intervención (Carbone, 2005). Sin embargo, la prueba obtenida de la intervención de las comunicaciones solo se considerará lícita si cumple con los requisitos establecidos en el artículo 2.10 de la Constitución Política y los artículos 230 del Código Procesal Penal (CPP); de lo contrario, nos encontraríamos ante una prueba ilícita (Rosas, 2016).

Es fundamental señalar que la finalidad de la intervención es obtener elementos de convicción que sirvan como medios de prueba en la etapa de juicio. No obstante, es necesario ser cuidadosos, ya que si los requisitos mencionados anteriormente no se cumplen, la prueba puede considerarse ilícita. En este sentido, San Martín (2015) sostiene que cualquier fuente de prueba (obtenida) que vulnere derechos fundamentales invalida la prueba, lo que lleva a su prohibición de valoración probatoria. Este criterio es compartido por el Tribunal Constitucional (TC), que considera como prueba prohibida aquella que se

obtiene violando directa o indirectamente derechos fundamentales (STC Exp. N° 00655-2010-PHC/TC).

Por otro lado, Bustamante (2001) señala que no es suficiente que la prueba haya sido obtenida infringiendo una norma con rango de ley para ser considerada ilícita, sino que debe lesionar un derecho fundamental con el cual el derecho de prueba guarde relación de manera ilegal.

Nuestra Constitución Política, en su artículo 2.10, no solo establece el derecho al secreto de las comunicaciones, sino también la excepción a esta regla, es decir, la restricción de dicho derecho con el fin de obtener medios probatorios en procesos penales. Esta restricción legal se complementa con los artículos 230 y 231 del CPP, así como otras leyes especiales.

Por tanto, el debido proceso garantiza que los medios probatorios que infrinjan un derecho fundamental no sean admitidos ni valorados, ya que de lo contrario el proceso no cumpliría con todas las garantías (Villegas, 2016). Es necesario analizar si la intervención se realizó de acuerdo con lo establecido en la ley, especialmente en la norma constitucional; de lo contrario, se estarían vulnerando derechos fundamentales.

Es importante precisar que el TC ha establecido que la prueba obtenida es lícita cuando existe autorización de uno de los interlocutores, y estos tienen dominio sobre la comunicación, lo cual abarca el registro y su contenido sin afectar este derecho. Por lo tanto, la prueba obtenida con dicha autorización no constituye una prueba ilícita (Exp. N° 00867-2011-PA/TC).

2.2.1.13 Finalidad del levantamiento del secreto de las comunicaciones. La finalidad inmediata de la intervención de las comunicaciones es investigar una hipótesis

delictiva, verificando la veracidad de las afirmaciones y la posible vinculación de una persona específica con el hecho delictivo (Carbone, 2008). Esto implica sacrificar un derecho fundamental en aras de cumplir con la finalidad constitucional de obtener elementos de convicción para la investigación de un delito y la identificación de posibles implicados (Casanova, 2014).

Esta finalidad se sustenta en el uso de técnicas especiales de investigación como la intervención de las comunicaciones, que incluye la interceptación, registros históricos, mensajes de texto, geolocalización y acceso a comunicaciones por correo electrónico u otros medios, con el objetivo de cumplir su propósito (Castillo, 2022).

En este contexto, sostengo la posición de que los tribunales no deben ordenar intervenciones telefónicas de manera genérica, arbitraria o indiscriminada, ni basadas en sospechas vagas. Dichas intervenciones deben ser ordenadas basándose en sospechas concretas y con fines específicos, considerando la necesidad de la medida y los objetivos que se espera alcanzar, ya que su finalidad es obtener información concreta que pueda ayudar en la investigación, recolectando elementos de convicción específicos de acuerdo con la sospecha fiscal.

Entonces, ¿cuál es la finalidad del levantamiento del secreto de las comunicaciones? La respuesta inmediata es obtener elementos de convicción que respalden la teoría del delito del fiscal. Al profundizar en esta respuesta, podemos afirmar que la finalidad de esta medida incluye identificar a los autores y/o partícipes, determinar la responsabilidad penal y recopilar fuentes de prueba que puedan utilizarse en la etapa de juicio, o descartarlas en caso contrario.

2.2.1.14 Aplicación del test de proporcionalidad. Para evaluar las medidas restrictivas que puedan afectar cualquier derecho fundamental y evitar que estas sean abusivas o arbitrarias, se utiliza el mecanismo constitucional denominado test de proporcionalidad. Este mecanismo debe entenderse como el equilibrio entre el fin perseguido y la restricción de un derecho fundamental, donde la medida debe superar un filtro: solo cuando esté debidamente justificada se podrá sacrificar el derecho fundamental de manera estrictamente necesaria y proporcional.

La finalidad del test de proporcionalidad es ponderar la restricción del derecho con el beneficio que aporta al interés público y determinar si debe primar sobre el interés del titular del derecho (Marco Urgell, 2010). Por otro lado, Bernal (2003) señala que el principio de proporcionalidad se compone de tres subprincipios:

- Idoneidad: La intervención debe ser adecuada para alcanzar un fin legítimo.
- Necesidad: Toda intervención al derecho fundamental debe ser la más benigna entre todas las que son adecuadas para alcanzar un mismo fin.
- Proporcionalidad en sentido estricto**:** La relación entre el objetivo perseguido y los derechos fundamentales; es decir, las ventajas obtenidas con la intervención o restricción del derecho deben compensar equitativamente los sacrificios que esta implica para los titulares del derecho.

En nuestra legislación, el test de proporcionalidad debe estar debidamente motivado en la resolución judicial (Díaz, 2006), desarrollando los tres subprincipios mencionados. Esto implica tener en consideración (a) Idoneidad; (b) Necesidad; y (c) Proporcionalidad (equilibrio entre medio y fin).

Asimismo, nuestro CPP en el artículo VI del Título Preliminar establece que las medidas restrictivas de derechos deben cumplir con la legalidad y estar debidamente motivadas en las resoluciones judiciales que las autorizan, en consonancia con la naturaleza y finalidad de la medida, respetando el principio de proporcionalidad.

El Tribunal Constitucional (TC) señala que el procedimiento para aplicar el test de proporcionalidad en decisiones que afectan derechos fundamentales debe seguir tres juicios:

(a) Juicio de idoneidad. La restricción del derecho debe ser adecuada y pertinente para alcanzar la finalidad buscada.

(b) Juicio de necesidad. Verificar si existen medios alternativos para lograr el mismo fin

(c) Juicio de ponderación. Se realiza cuando se han superado los dos juicios anteriores, comparando y equilibrando los principios constitucionales en conflicto.

Cuando una medida restrictiva de intensidad leve logra niveles elevados de satisfacción, se concluye que ha superado el test de proporcionalidad y constituye una restricción legítima a derechos constitucionales. Es esencial contrastar el grado de afectación de un derecho con el nivel de satisfacción que se logra con los objetivos perseguidos por la intervención. Esta intensidad en las medidas restrictivas puede describirse como grave, media o leve, y sus resultados en términos de satisfacción pueden ser elevados, medios o débiles (STC 0045-2005-PI/TC - Lima).

En resumen, el test de proporcionalidad, en su último subprincipio, establece que el grado de afectación de una medida restrictiva debe ser equivalente al beneficio que se obtiene con los resultados de su ejecución.

2.3 Fraude informático

2.3.1 Antecedentes

Con el paso de los años, los avances tecnológicos en información y comunicación han evolucionado de manera acelerada, brindándonos servicios relacionados con el procesamiento, almacenamiento y transmisión de datos, además de facilitar la comunicación a través de internet, una red mundial de información y comunicación. Estos avances tecnológicos contribuyen a la integración cultural, social y económica a nivel global, creando nuevas formas de interacción. Sin embargo, junto con estos avances vienen también los riesgos, como los delitos informáticos, que interfieren ilegalmente en sistemas informáticos y en internet.

En respuesta a estos desafíos, el poder legislativo ha promulgado la Ley de Delitos Informáticos (Ley Nº 30096), cuya finalidad es prevenir y sancionar conductas ilícitas que afectan a datos informáticos, sistemas y otros bienes jurídicos mediante el uso de tecnologías de información y comunicación.

Según la doctrina, los delitos informáticos son acciones ilícitas que eluden los sistemas de seguridad de dispositivos electrónicos, como intrusiones en computadoras, sistemas de datos o correos electrónicos mediante el uso de claves de acceso, entre otros. Estas conductas delictivas solo pueden llevarse a cabo a través de las Tecnologías de la Información y la Comunicación (TIC), que son el objetivo, el medio y/o el lugar de ejecución del delito (Villavicencio, 2014).

Por otro lado, Rayón y Gómez (2014) señalan que los ciberdelitos son infracciones punibles en las que está involucrado internet y equipos informáticos, siendo estos dispositivos electrónicos utilizados para cometer delitos.

Además, según Pérez (2019), existen tres teorías para definir los delitos informáticos:

(a) Concepción amplia. Se refiere al uso de computadoras como única característica distintiva.

(b) Concepción intermedia. Distingue el uso de computadoras como instrumento del delito y la informática (software) como objeto del delito.

(c) Concepción restringida o jurídica. Engloba todas las conductas dirigidas contra el software de la computadora que no pueden ser subsumidas en figuras delictivas tradicionales.

Mazuelos (2001) destaca que los delitos informáticos son autónomos en comparación con los delitos tradicionales. Es fundamental destacar que con el paso del tiempo han surgido nuevas modalidades de delitos informáticos, mientras que otros han evolucionado al ritmo del avance tecnológico, lo que genera una mayor complejidad en la detección y sanción de estos delitos. Las conductas asociadas a los delitos informáticos se crean y modifican al mismo ritmo que las nuevas tecnologías y su evolución (Vinelli, 2021).

La investigación de este tipo de delitos evoluciona al ritmo de la tecnología; sin embargo, las técnicas de investigación utilizadas por la policía y la fiscalía no siempre se desarrollan al mismo ritmo, especialmente debido a limitaciones como la falta de personal capacitado y el aumento constante de casos de delitos informáticos.

2.3.2 Convenio de Budapest

El Convenio sobre Ciberdelincuencia es un tratado internacional suscrito por los miembros del Consejo de Europa el 23 de noviembre de 2001 en Budapest, con el propósito de combatir los delitos informáticos mediante la cooperación internacional, la estandarización y la homologación de normas penales (Guerrero Argote, 2018).

En teoría, el Convenio de Budapest ofrece a sus miembros una serie de términos que facilitan la tipificación común de los delitos informáticos, establecen estándares mínimos a nivel procesal para posibilitar la persecución penal y obligan a los países miembros a cooperar y compartir información.

El desarrollo normativo en este tratado internacional representa el esfuerzo conjunto de los países miembros en la lucha contra la ciberdelincuencia. Es esencial destacar las partes de este tratado internacional, resaltando disposiciones clave y su importancia global en ciberseguridad.

En este sentido, el Convenio de Budapest aborda los siguientes puntos (Acurio, 2016):

- El preámbulo, que establece como finalidad la estandarización de la normativa contra la ciberdelincuencia entre los países miembros y promueve la cooperación internacional.
- El capítulo uno, donde se definen conceptos clave.
- El capítulo dos, que aborda la parte sustantiva del derecho penal contra la ciberdelincuencia, así como la obligación de los países miembros de adoptar las medidas necesarias. También incluye aspectos procesales que establecen condiciones y garantías.
- Las disposiciones finales

Dentro del capítulo dos de este tratado internacional se prescriben aspectos sustantivos y procesales. Por ejemplo, el artículo ocho define el delito de fraude informático como aquel acto que causa daños patrimoniales a terceros mediante la manipulación y/o interferencia de datos informáticos.

La parte procesal, desarrollada desde el artículo 14 hasta el 21, tiene como finalidad la búsqueda de información relevante a través de datos informáticos en la lucha contra la ciberdelincuencia. Esto incluye la conservación de datos informáticos, así como la presentación de estos por parte del titular y/o proveedor de servicios de datos informáticos bajo su control, el registro y acceso a información de datos informáticos (intervención de las comunicaciones a nivel histórico), y finalmente, la obtención en tiempo real de datos informáticos (interceptación de las comunicaciones).

Los beneficios obtenidos al integrarse al Convenio de Budapest atrajeron la atención a nivel mundial, lo que ha llevado a un aumento en el número de sus miembros con el paso de los años, incluyendo la integración de nuestro país en 2019. Por este motivo, Perú no fue ajeno a la normativización de los delitos informáticos, que fueron derogados por la Ley N° 30096 (Ley de Delitos Informáticos), normativa que actualmente está en vigencia. Además, nuestro país se adhirió al Convenio de Budapest en 2019.

2.3.3 Delito de fraude informático

2.2.3.1 Elementos estructurales del tipo.

Sujeto Activo. El sujeto activo es la persona que ejecuta la conducta típica en un delito. Los delitos pueden clasificarse en impropios, cuando cualquier persona tiene la capacidad de cometer la conducta ilícita, y propios, cuando solo ciertas personas tienen la capacidad de cometer el ilícito (Peña y Almanza, 2010).

En el caso del delito de fraude informático, puede ser cometido por cualquier individuo que tenga conocimientos de informática y realice acciones fraudulentas a través de medios informáticos. Estos individuos pueden incluir hackers, programadores malintencionados, entre otros.

Sujeto Pasivo. El sujeto pasivo es el titular del interés jurídico lesionado o puesto en peligro, identificado respondiendo a la pregunta "¿Quién es el titular del bien?" (Peña y Almanza, 2010).

En el caso del fraude informático, el sujeto pasivo suele ser una entidad o persona que sufre pérdidas o daños como resultado del ilícito penal. Esto puede incluir personas naturales o jurídicas, organismos estatales u cualquier entidad que sea objetivo del fraude informático y sufra perjuicios patrimoniales.

Objeto del Delito. El objeto material del delito de fraude informático es el patrimonio sobre el cual recae el perjuicio, es decir, el desplazamiento patrimonial que se lleva a cabo mediante un sistema informático (Mayer y Oliver, 2020).

Elementos Objetivos del tipo. La ley de delitos informáticos prescribe en su artículo 8 el delito de fraude informático, describiendo la siguiente conducta punible: "El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático". Este tipo penal aborda muchas modalidades delictivas, ya que contiene una cantidad considerable de modalidades en un mismo tipo penal, entre las que se incluyen el phishing, pharming, espionaje informático o hacking, y sabotaje informático, entre otros.

Vinelli (2021) sostiene que para que se configure este tipo penal, es necesaria y obligatoria la manipulación de sistemas de información con el fin de obtener un provecho patrimonial o económico, sin requerir el uso de amenazas o violencia. Una de las características de este delito es la conducta engañosa utilizada para lograr su fin.

La acción material del delito de fraude informático no recae sobre el hardware (parte física de la computadora), sino en la intrusión en el software (soporte lógico de un sistema informático en programas que ejecutan actividades específicas). En este sentido, debemos comprender que en algunos casos, los sistemas informáticos constituyen el objeto material del delito, mientras que en otros casos son solo un instrumento para cometer el hecho delictivo. Este tipo penal tiene la peculiaridad de no exigir que la defraudación preceda a un desplazamiento patrimonial como consecuencia del engaño, por lo que el delito de fraude informático no está sujeto a los requisitos exigidos en el clásico delito de estafa (Pérez, 2019).

En este sentido, Villavicencio (2014) expresa que el delito de fraude informático penaliza un conjunto de conductas, entre las cuales se incluyen: (a) diseñar, proyectar o planificar; (b) alterar, dañar, descomponer; (c) borrar, desaparecer o quitar; (d) suprimir o hacer desaparecer; (e) clonar o producir clones, en el funcionamiento de sistemas informáticos con el fin de obtener un beneficio para sí mismo o para un tercero. Este es un delito de resultado, ya que para su configuración se necesita un resultado separado de la conducta que cause daño a un tercero.

Como hemos podido observar, este delito resulta ser genérico, permitiendo la existencia de diversas modalidades en las conductas delictivas que configuran el tipo, y estas modalidades evolucionan al mismo ritmo que el avance tecnológico, lo que representa

un gran problema en la investigación de estos delitos debido a las limitaciones por el desconocimiento a nivel tecnológico por parte de los operadores de justicia, fiscalía y la policía nacional, así como las limitaciones en la investigación preparatoria.

En este sentido, Mayer y Oliver (2020) describen algunas modalidades de fraudes informáticos, entre las cuales se incluyen: (a) phishing, que consiste en obtener de manera fraudulenta datos personales, cuentas bancarias y tarjetas de crédito para realizar transacciones; (b) pharming, que implica la creación de sitios web falsos con el fin de obtener datos (personales y/o bancarios); (c) espionaje informático o hacking; y (d) sabotaje informático, que son modalidades preparatorias para la realización del delito de fraude informático, ya que con estas herramientas ilícitas logran obtener datos de manera ilegal para obtener beneficios económicos.

Existen diversas modalidades en las que los criminales informáticos utilizan para obtener datos de manera ilegal o ilícita, datos que serán usados para causar un perjuicio patrimonial en sus víctimas en beneficio propio. Con el tiempo, los avances tecnológicos aumentan, lo que obliga a los ciberdelincuentes a adaptarse y crear nuevas modalidades delictivas que se encuentran dentro del tipo penal de fraude informático.

***Elementos subjetivos del tipo*.** El delito de fraude informático es un delito doloso, requiriendo la comprensión del conocimiento de la falta de autorización para realizar la intrusión en los sistemas informáticos, así como el animus lucrandi o ánimo de lucro, ya que el sujeto activo busca obtener ilegalmente un beneficio económico (Pérez, 2019). La conducta derivada del delito de fraude informático se basa en la tendencia interna trascendente que busca satisfacer el fin lucrativo a través de medios informáticos.

Es importante destacar que este tipo penal solo admite el dolo directo para su configuración, ya que implica el conocimiento de la falta de autorización por parte del titular de los datos a los que el sujeto activo accede mediante diferentes mecanismos informáticos, muchos de los cuales son ilegales. Esto solo se logra con un conocimiento avanzado por parte del sujeto activo sobre los sistemas informáticos. Además, la finalidad de esta conducta es el animus lucrandi, es decir, obtener beneficios económicos mediante la intrusión ilegal en datos informáticos.

2.2.3.2. Bien jurídico protegido. Se ha debatido si los delitos informáticos protegen un bien jurídico común, a esto Kleiman y Tello (2018) expresan su posición al señalar que los delitos informáticos al ser cometidos mediante sistemas informáticos y la internet, empero esto no serían bienes jurídicos protegidos, si no por el contrario serian medios para cometer delitos tradicionales, no variando ni implementando la protección de un nuevo bien jurídico, este criterio es adoptado por la preocupación de los autores por la sobre criminalización en la modernización del Código Penal Argentino (Defensoría del Pueblo, 2023)

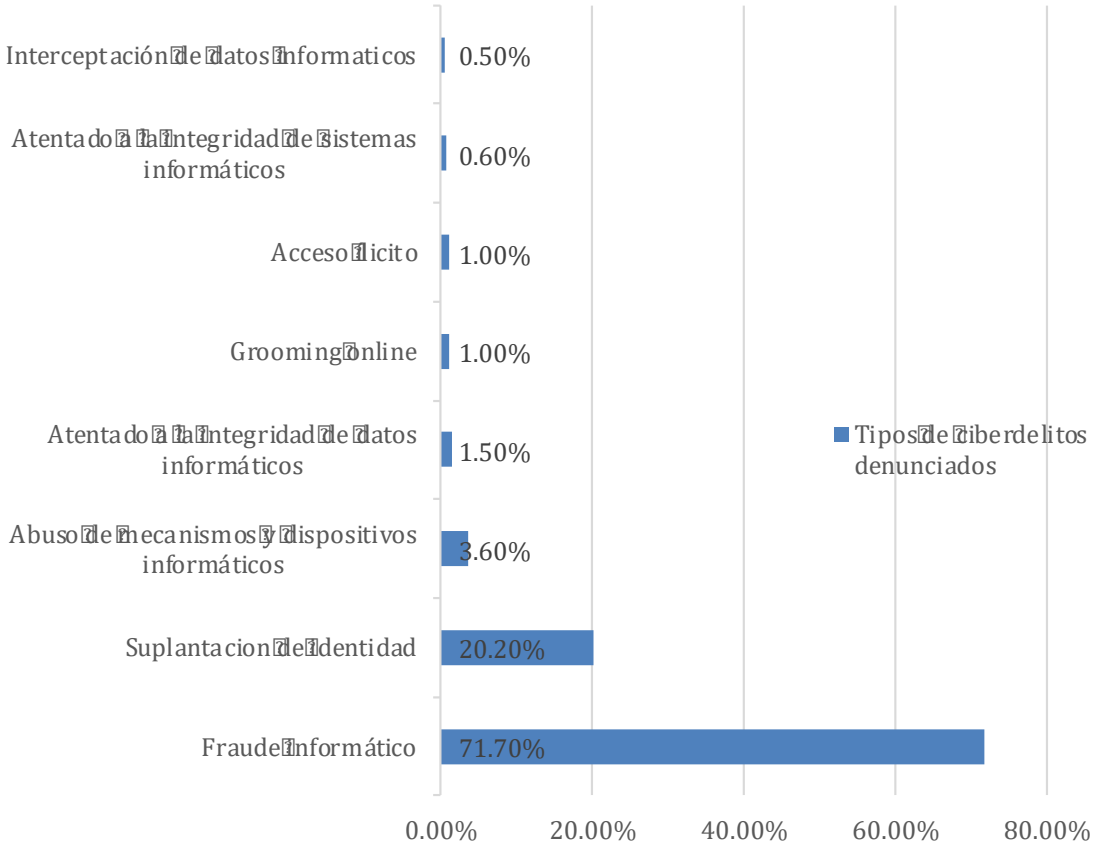
Sin embargo, el delito de fraude informático, al implicar la utilización e intrusión en datos y sistemas informáticos para llevar a cabo delitos convencionales, afecta tanto el derecho a la protección de datos informáticos como el derecho a la intimidad personal. Por lo tanto, se puede considerar que uno de los bienes jurídicos protegidos por los delitos informáticos en general es la salvaguarda de los datos informáticos y la privacidad. El bien jurídico protegido en el delito de fraude informático es la preservación del patrimonio económico del sujeto pasivo del delito sobre las bases de los datos y sistemas informáticos respecto a su adecuado funcionamiento (Pérez, 2019).

Concluimos que para el delito de fraude informático el bien jurídico convencional es el patrimonio, mientras que surge por la introducción, diseño, alteración, supresión y/clonación de datos informáticos para cometer este delito es la protección de datos informáticos.

2.2.3.3 Modalidades recurrentes en el delito de fraude informático. El delito de fraude informático involucra verbos rectores como introducir, diseñar, alterar, borrar, suprimir y clonar datos informáticos, lo que conlleva a la posibilidad de generar múltiples modalidades que se subsumen en este tipo penal. El delito de fraude informático es el delito informático más denunciado a nivel nacional, representando el 71.7 % del total de ciberdelitos denunciados en 2021.

Figura 2

Tipos de ciberdelitos denunciados

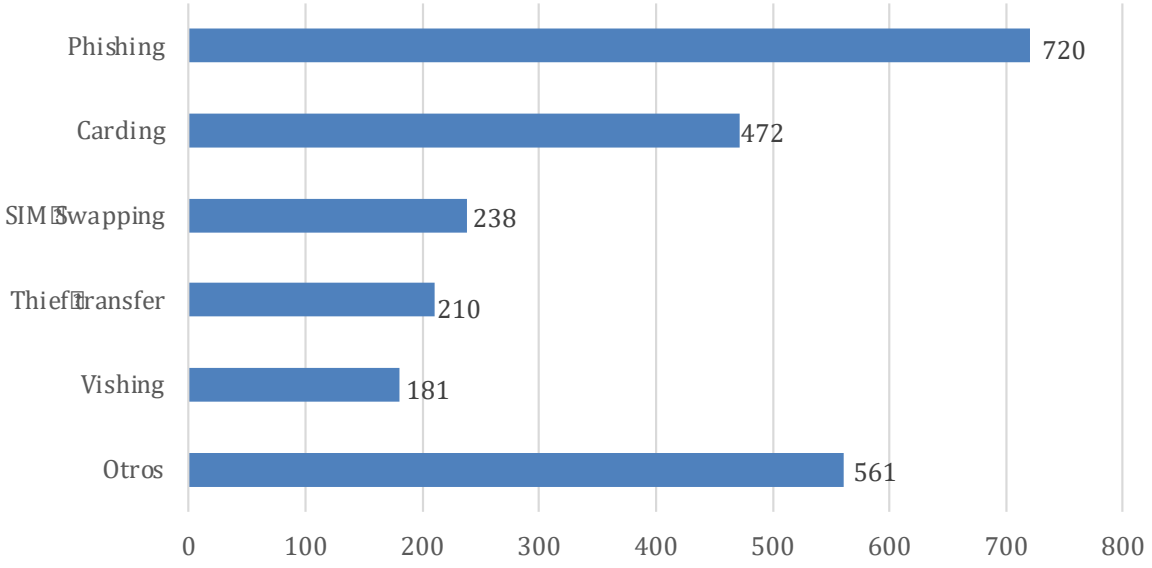


Nota. Los datos fueron recogidos del Sistema Informàtico de Registro de Denuncias de Investigación Criminal (SIRDIC) de la Policía Nacional del Perú, en la que se muestra el porcentaje de delitos informáticos cometidos en el Perú el 2021.

Es así que, según la investigación de datos recopilados por la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), se registraron un total de 3,946 denuncias por delitos informáticos, de las cuales 2,382 correspondieron a fraude informático. Entre las principales modalidades utilizadas para cometer este último delito se encuentran: (a) phishing; (b) carding; (c) SIM swapping; (d) transferencias fraudulentas; y (e) vishing (El Peruano, 2023).

Figura 3

Denuncias por modalidades de fraude



Nota. Los datos fueron recogidos de la Division de Investigacion de Delitos de Alta Tecnologia (DIVINDAT), en la que se muestra el número de delitos de fraude informático cometidos en el Perú.

Phishing y pharming. El *phishing* consiste en simular ser entidades bancarias para solicitar a los usuarios sus datos y claves de tarjetas bancarias a través de formularios o correos electrónicos que contienen enlaces a páginas web falsas similares a las originales. El objetivo es realizar transferencias y retiros fraudulentos (Martínez, 2018).

Por otro lado, el *pharming* suplanta el sistema de nombres de dominio (DNS) redirigiendo al usuario a un sitio web falso para apoderarse de sus contraseñas. Cuando un usuario ingresa una dirección web, esta se convierte en una dirección numérica de Protocolo de Internet (IP) mediante el DNS (Fernández, 2014).

Esta modalidad implica la intrusión en el sistema del usuario y la modificación del sistema de resolución de nombres. De esta manera, cuando el usuario intenta acceder a un sitio web en línea, en realidad está ingresando a la dirección IP de una página web fraudulenta.

En ambos casos, el objetivo de estas modalidades es obtener datos personales (nombre, número telefónico, DNI y contraseñas) para beneficios patrimoniales mediante transferencias bancarias, compras en línea, entre otros.

Carding. El *carding* es un procedimiento utilizado por los clonadores a través de la web o cajeros automáticos. Su objetivo es confirmar el saldo de las tarjetas clonadas realizando compras con montos reducidos para no alertar a la víctima (Martínez, 2018).

Los ciberdelincuentes obtienen acceso no autorizado a tarjetas bancarias de terceros para realizar transacciones de importes reducidos. También utilizan la identidad de individuos con buen historial crediticio y fondos, empleando sus tarjetas para efectuar compras significativas en plataformas de comercio electrónico internacionales.

SIM Swapping. Bajo esta modalidad, se obtiene un duplicado de la tarjeta SIM de un cliente bancario al recopilar información confidencial. Al activar el duplicado, la línea telefónica original queda inoperable, lo que permite acceder a datos personales y cuentas bancarias para realizar compras y transferencias no autorizadas (Sifuentes, 2022).

Los ciberdelincuentes adquieren información personal de terceros, bloquean y duplican la tarjeta SIM mediante contactos con empresas de telefonía. Esto les permite utilizar los datos obtenidos para acceder a las cuentas de banca móvil de las víctimas, realizando transacciones como transferencias y solicitudes de préstamos, entre otras acciones fraudulentas.

Thief Transfer. Este método implica el uso de teléfonos móviles robados o extraviados para llevar a cabo fraudes informáticos. Los criminales extraen la tarjeta SIM del dispositivo móvil bloqueado debido a robo o pérdida y la insertan en otro aparato para acceder a toda la información almacenada y perpetrar el fraude.

Vishing. En este tipo de estafa, la persona afectada es engañada mediante llamadas telefónicas en las que el estafador falsamente toma la identidad de una empresa, entidad o individuo de confianza. El propósito es obtener datos personales y confidenciales de la víctima.

2.2.3.5 El delito de fraude informático y medios especiales de investigación. Es indudable que la ciberdelincuencia no puede combatirse utilizando métodos tradicionales o convencionales, ya que requiere de métodos especiales de investigación como la intervención de las comunicaciones o el levantamiento del secreto bancario, ambos con especial relevancia cuando se trata de delitos informáticos contra el patrimonio, como el fraude informático.

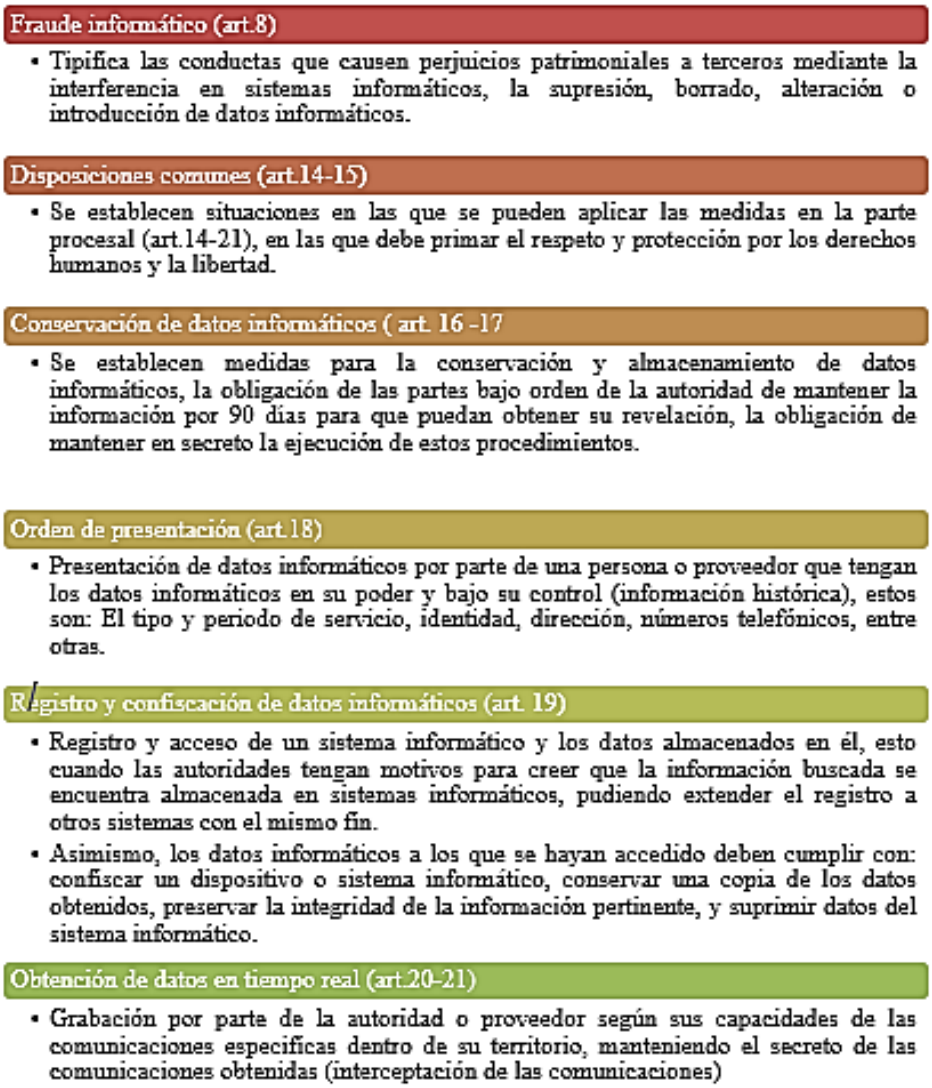
Esto no significa que en todos los casos se deba autorizar la intervención de las comunicaciones; más bien, debe primar la necesidad y finalidad de la medida sobre el grado de afectación del derecho fundamental, utilizando el test de proporcionalidad.

Podemos destacar que la propuesta del Convenio de Budapest en la lucha contra la ciberdelincuencia incluye la investigación con intervención de las comunicaciones en las redes informáticas, telecomunicaciones y comunicaciones, siempre respetando los derechos humanos y las libertades.

En este sentido, podemos señalar que en la investigación del delito de fraude informático se establecen pautas no solo a nivel nacional, como las prescritas en el artículo 8 y las disposiciones generales de la Ley N° 30096 (Ley de Delitos Informáticos), donde se evidencia la necesidad del uso de la intervención de las comunicaciones para obtener información relevante en la investigación y en la lucha contra la ciberdelincuencia, sino también en tratados internacionales como el Convenio de Budapest, que reconoce la intervención de las comunicaciones como necesaria en la lucha contra la ciberdelincuencia y, específicamente, en el delito de fraude informático.

Figura 4

Comparativa del aspecto procesal del Convenio de Budapest



Nota: Elaboracion propia. Se muestra la descripcion del aspecto procesal del convenio de Budapest.

CAPÍTULO III: Diseño metodológico

3.1. Metodología

Las reglas metodológicas no son rígidas, sino plásticas, ya que no son normas intocables que encierren una verdad absoluta. La metodología nos ayuda a encontrar verdades y nos previene de posibles errores. Se trata, sin duda, de un conjunto de herramientas que asisten al investigador. Además, según Ramos (2018): La metodología describe y regula los diversos métodos. Es progresiva porque es autocorrectiva. La metodología no es irreversible ni un manual de recetas, sino un conjunto orgánico de procedimientos mediante los cuales: (a) se plantean los problemas científicos; y (b) se ponen a prueba las hipótesis científicas.

Por lo tanto, toda investigación requiere de un desarrollo metodológico, que representa el esqueleto moldeable para su desarrollo, con el fin de trabajar con rigurosidad científica y obtener resultados fiables.

3.1.1 Método dogmático

Se aplicó el método dogmático, ya que proporcionó un sentido conceptual al buscar la naturaleza jurídica de las normas procesales y leyes especiales que forman parte del problema general de esta tesis. La investigación de los dogmas tiene una sola explicación, la de servir al fin teórico de ayudar al intérprete a entender los institutos jurídicos y al fin práctico de hacer posible la explicación de las normas de la manera más adecuada a las exigencias del caso concreto. Ramos (2018)

Este enfoque describe, explica y justifica la naturaleza jurídica del levantamiento del secreto de las comunicaciones como técnica especial de investigación en el delito de fraude informático.

3.1.2. Método sociológico funcional

Esta investigación no se limitó únicamente a los conocimientos propios del derecho objetivo o formal, descritos en las normas, sino que también se contrastó con la realidad. Ramos (2018) explica que el método sociológico funcional intenta realizar un diagnóstico sobre la conformidad o discrepancia entre el orden jurídico abstracto y el orden social concreto, ya que la realidad no se conoce a través de la ley, sino a través de las manifestaciones humanas en el ámbito jurídico.

Por lo tanto, esta tesis obtuvo criterios reales mediante la técnica de entrevista escrita a tres fiscales y tres jueces de investigación preparatoria, quienes son competentes para conocer los casos de levantamiento del secreto de las comunicaciones en el delito de fraude informático. El objetivo fue contrastar los criterios utilizados para requerir y autorizar dicha medida.

3.2. Enfoque

Esta investigación se desarrolló bajo un enfoque cualitativo, acorde con la naturaleza de la investigación jurídica. Según Croda y Abad (2016), las técnicas de enfoque cualitativo permiten una comprensión integral de los marcos normativos, abordando aspectos dogmáticos, interpretativos, exegéticos, comparativos, sistemáticos y, en algunos casos, casuísticos. Este enfoque resulta altamente apropiado para avanzar en la presente investigación, ya que contribuye tanto a su desarrollo como a la obtención de resultados, al considerar las experiencias y situaciones específicas de individuos y grupos sociales.

El enfoque cualitativo se centra en las ciencias sociales y resulta el más adecuado para cumplir con los objetivos planteados en esta investigación. Se empleó la entrevista como técnica de recolección de datos con jueces y fiscales, para abordar el tema del levantamiento del secreto de las comunicaciones en el contexto del delito de fraude informático. Esto permitió evidenciar la realidad del problema y considerar diferentes perspectivas en el análisis.

3.3 Diseño de la investigación

El diseño de investigación comprende el conjunto de técnicas y métodos que se utilizan de manera lógica en el desarrollo de la investigación, con el propósito de otorgarle un orden coherente y garantizar su eficiencia. Este diseño se caracteriza por ser flexible, dialéctico, interactivo y reflexivo (Escudero y Cortez 2018).

En la investigación cualitativa, el diseño busca establecer formas de aproximación al problema para su explicación; la información recopilada debe ser sistematizada de manera clara y coherente (Guerrero y Guerrero, 2014).

3.3.1 Propósito intrínseco

El propósito intrínseco de la investigación consiste en determinar los objetivos que se persiguen en un estudio, definiendo así el propósito mismo de la investigación. Bajo este criterio, se identifican varios tipos de investigación: (a) descriptiva; (b) explicativa; (c) correlacional; y (d) exploratoria (Ríos, 2019).

En este estudio, se utilizó principalmente un enfoque descriptivo y explicativo. Según Ríos (2019), la investigación descriptiva tiene como objetivo principal describir situaciones, contextos, fenómenos o eventos. Por otro lado, la investigación explicativa

busca comprender las causas o motivos detrás de los fenómenos observados, profundizando en su análisis e interpretación para delimitar el alcance de la investigación.

En este contexto, la investigación se centró en describir cómo la falta de autorización para la intervención de las comunicaciones en casos de fraude informático, sin cumplir con el requisito de *suma pena*, afecta el desarrollo del proceso. Además, se exploraron las causas de esta problemática a través del análisis normativo y los criterios adoptados por jueces y fiscales que manejan casos de intervención de las comunicaciones en este tipo de delitos, obtenidos mediante la técnica de la entrevista.

3.3.2 Propósito extrínseco

El propósito extrínseco de la investigación se refiere al impacto que se espera tener en la comunidad jurídica una vez que se publique y transcurra el tiempo. Bajo este criterio, se distinguen dos tipos de investigación: (a) aplicada; y (b) teórica o pura (Ríos, 2019).

En este estudio, se adoptó un enfoque de investigación teórica o pura. Este tipo de investigación tiene como objetivo aplicar el conocimiento generado en esta tesis para abordar el problema de la negativa a autorizar la intervención de comunicaciones en casos de fraude informático cuando no se cumple con el requisito de *suma pena*. Los nuevos conocimientos derivados de esta investigación pueden ser utilizados para proponer cambios normativos y soluciones prácticas a esta problemática.

3.4. Población y muestra

Se recopiló información sobre el levantamiento del secreto de las comunicaciones mediante preguntas abiertas plasmadas en cuestionarios dirigidos a jueces y fiscales que tienen experiencia laboral en la intervención de comunicaciones. Para ello, se establecieron los siguientes criterios:

Criterios de inclusión.

Se incluyeron tres jueces de investigación preparatoria y tres fiscales del distrito judicial y fiscal de Junín que tienen conocimiento sobre casos relacionados con el delito de fraude informático y el levantamiento del secreto de las comunicaciones.

Criterios de exclusión.

No se consideraron especialistas, asistentes jurisdiccionales ni asistentes fiscales que tengan experiencia en el ámbito de levantamientos del secreto de las comunicaciones.

Es importante señalar que inicialmente se solicitó acceso a diez expedientes judiciales relacionados con levantamientos del secreto de las comunicaciones en procesos por fraude informático. Sin embargo, el módulo penal de la CSJJU rechazó esta solicitud debido a que los procesos están bajo reserva. A pesar de esto, se obtuvieron criterios sobre el levantamiento del secreto de las comunicaciones a través de entrevistas con los fiscales que lo solicitan y los jueces de investigación preparatoria de la CSJJU que autorizan esta medida.

El objetivo fue determinar el tratamiento histórico del levantamiento del secreto de las comunicaciones en casos de fraude informático, considerando el marco normativo que lo regula y aplicando el test de proporcionalidad para determinar los criterios de lesividad.

3.5. Técnicas e instrumentos de investigación para el recojo de información

Según Ñaupas et al. (2018), las técnicas de investigación son un conjunto de normas y procedimientos que regulan un proceso determinado con el fin de alcanzar un objetivo específico, mientras que los instrumentos son herramientas materiales o conceptuales mediante las cuales se recopilan datos e información. En conjunto, la técnica y el

instrumento tienen como finalidad la búsqueda y clasificación de información relevante y confiable para el desarrollo de la investigación.

En este contexto, esta investigación utilizó la técnica de la entrevista escrita, la cual facilitó la recopilación y clasificación de información con la ayuda de expertos en la materia (jueces y fiscales).

Como instrumento se empleó una guía de entrevista para sistematizar las preguntas en un orden secuencial y permitir que los entrevistados plasmaran sus respuestas. Esto facilitó la recolección, síntesis y almacenamiento de la información obtenida a través de los instrumentos de recopilación de datos.

Para organizar, procesar, sintetizar y contrastar la información obtenida de las entrevistas, se aplicó la técnica de triangulación de datos, como menciona Hernández (2018). Esta técnica permitió confirmar y corroborar los datos obtenidos en las entrevistas para validar la información recopilada. Todos los datos obtenidos en las entrevistas se registraron en un cuadro, donde se realizó el análisis y la síntesis de los resultados de cada pregunta.

Finalmente, para el desarrollo del marco teórico se sistematizó la información proveniente de libros, enciclopedias y revistas especializadas en la materia. Estas fuentes de información permitieron crear un repositorio de datos para sintetizar la información en la tesis de investigación (Ramos, 2018).

3.6. Recopilar información

Para llevar a cabo la investigación y obtener una comprensión más profunda de la realidad en torno al levantamiento del secreto de las comunicaciones en el delito de fraude

informático, se utilizó la técnica de la entrevista con la ayuda de una guía de preguntas dirigida a jueces y fiscales especializados en estos casos.

En cuanto al desarrollo del marco teórico, se recopiló información principalmente sobre los temas relacionados con el levantamiento del secreto e inviolabilidad de las comunicaciones, así como del delito de fraude informático, además de otros temas que puedan contribuir a la investigación. Para ello, se aplicaron los siguientes criterios:

Tabla 3

Fuentes de Información Teórica

Libros	**Tesis y artículos científicos**	**Videos**	**Jurisprudencia**
El recojo de información de libros debe realizarse de las principales editoriales peruanas o extranjeras, así como de autores reconocidos en el ámbito jurídico, asimismo deben ser especializados en el tema a investigar. Estos pueden ser libros físicos y/o recogidos de páginas web.	La información por recogerse debe ser extraída de repositorios confiables como: (a) Scielo, (b) Renati, (c) repositorios de universidades reconocidas que cuenten con certificación Digital Object Identifier (DOI).	Videos de conferencias magistrales de los que se recogerá información respecto al tema, así como videos publicados por la Academia de la Magistratura, Poder Judicial y Ministerio Público.	Se tomará en cuenta la jurisprudencia nacional emitida por la CSJR y el TC. Asimismo, de las sentencias de la Corte IDH y eventualmente de jurisprudencia comparada.

Nota: Elaboración propia. En la presente tabla se muestra las fuentes a usarse para obtener información teórica de la tesis.

CAPÍTULO IV: Resultados y discusión

4.1. Resultados

Como se detalló en la sección metodológica, en las entrevistas realizadas a los jueces de los JIP de Huancayo y a los fiscales de la Fiscalía Penal Corporativa de Huancayo, se obtuvieron los siguientes resultados. Para esto, se empleó la técnica de triangulación, la cual consiste en contrastar diferentes fuentes para corroborar los hallazgos, mejorar la validez y proporcionar una visión más integral de un tema en particular.

Tabla 4

Definiciones sobre el levantamiento del secreto de las comunicaciones

Fiscal: Mario Grover Orellana Castillo	**Fiscal: Luis Álvaro Cárdenas Moreno**	**Fiscal: Elías Salcedo Ordaya**
El secreto de las comunicaciones es una obligación de carácter constitucional, por la cual todas las empresas de telecomunicaciones se encuentran obligadas a adoptar medidas y procedimientos razonables para proteger la inviolabilidad de las comunicaciones. En esa línea de entendimiento y considerando que ningún	Es una medida limitativa de derechos que permite a los operadores de justicia buscar información protegida por el derecho al secreto de las comunicaciones. Actualmente, esta medida se utiliza con frecuencia en casos de mayor complejidad, como la ciberdelincuencia.	Es una medida coercitiva que faculta al juez, quien, previo requerimiento del fiscal ordena el levantamiento del secreto de las comunicaciones con la finalidad de lograr el éxito de alguna investigación.

derecho es absoluto, las comunicaciones, telecomunicaciones o sus instrumentos solo pueden ser abiertos, incautados, interceptados o intervenidos por orden motivada del Juez, con las garantías previstas en la ley.		
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
La intervención de las comunicaciones telefónicas supone una interferencia en el derecho fundamental de la persona investigada, la cual solo podrá acordarse en el marco de una investigación penal con el fin de perseguir delitos graves y siempre bajo control judicial.	El levantamiento del secreto de las comunicaciones es un método especial de investigación que consiste en obtener datos del contenido de estas, siempre que el caso en concreto lo amerite, con la finalidad de que la investigación obtenga resultados (elementos de convicción). Asimismo, constituye una medida restrictiva del derecho fundamental al secreto de las comunicaciones, por lo que debe ser tratada con cautela, teniendo en cuenta los requisitos procesales y el test de proporcionalidad.	Constituye la orden impartida por el juez de investigación preparatoria, previa solicitud fiscal debidamente motivada, con el fin de que las operadoras de telefonía proporcionen información histórica sobre las comunicaciones realizadas y recibidas por un imputado con sus coimputados, cómplices o terceros. Esta medida tiene como objetivo obtener información para

	esclarecer los hechos que se están investigando.

Los entrevistados conceptualizan la intervención de las comunicaciones como un método de investigación especial en el que se restringe el derecho al secreto de las comunicaciones con el objetivo de obtener elementos de convicción para esclarecer los hechos, delimitar responsabilidades e identificar al autor o coautores del delito. Esta medida restrictiva solo puede ser solicitada por el fiscal y ordenada por el juez competente.

Nota: Elaboración propia. Esta tabla se muestra los resultados de la primera pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas

Tabla 5

Definición de delitos informáticos y el delito de fraude informático en particular

Fiscal: Mario Grover Orellana Castillo	**Fiscal: Luis Álvaro Cárdenas Moreno**	**Fiscal: Elías Salcedo Ordaya**
Los delitos informáticos comprenden conductas en las cuales los sujetos activos se valen de programas informáticos para cometer infracciones, tales como la suplantación de sitios web, estafas, entre otros. En cuanto al fraude informático, este implica el uso de computadoras, Internet,	Los delitos informáticos engloban todas aquellas conductas típicas, antijurídicas y culpables que se cometen en el ámbito digital a través de las Tecnologías de la Información y la Comunicación (TIC). En este sentido, el delito de fraude informático constituye una	Es un delito poco estudiado y también de difícil aplicación debido a los conceptos en el campo tecnológico que los fiscales, jueces y abogados desconocen, lo cual implica la necesidad de capacitación por unidades especializadas.

dispositivos de internet y servicios de internet para defraudar, es decir, cualquier situación en la que se utilicen indebidamente datos bancarios y/o información personal con el fin de cometer delitos.	modalidad dentro de este tipo de delitos, específicamente del tipo replica, donde el bien jurídico protegido es tradicional es el patrimonio, y se ve amenazado a través de las TIC.	
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
El delito informático, también conocido como delito cibernético o ciberdelito, abarca todas las acciones que se realizan en el entorno digital, espacios digitales o en internet. Debido a la globalización digital de la sociedad, la delincuencia se ha expandido a esa dimensión. El fraude informático se encuentra previsto en el artículo 8 de la Ley 30056 y se imputa a aquel que, mediante el uso de tecnologías de la información o de la comunicación, lleva a cabo acciones fraudulentas.	Son conductas típicas, antijurídicas y culpables, en las cuales los sujetos utilizan programas informáticos para cometer delitos tradicionales. Estos delitos se encuentran previstos en una ley especial, la Ley de Delitos Informáticos. El delito de fraude informático es una infracción contra el patrimonio en la cual el sujeto activo hace uso de la tecnología con el fin de obtener un beneficio económico ilícito.	El delito informático es la acción ilegal delictiva que hace uso de dispositivos electrónicos e internet con el fin de vulnerar, sustraer o dañar bienes patrimoniales o no, ya sea de personas o entidades públicas o privadas. Considero que el delito de fraude informático es el comportamiento que afecta el software o soporte lógico de un sistema automatizado de la información.

Los entrevistados conceptualizan los delitos informáticos, o ciberdelitos, como toda acción típica, antijurídica y culpable que se lleva a cabo mediante el uso de software o soporte lógico de un sistema automatizado de la información. El delito de fraude

informático es una infracción contra el patrimonio en la cual, mediante el uso de la tecnología, se realiza interferencia o manipulación en el funcionamiento del sistema informático con el fin de obtener un provecho patrimonial ilícito.

Nota: Elaboración propia. Esta tabla se muestra los resultados de la segunda pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas

Tabla 6

El levantamiento del secreto de las comunicaciones es indispensable para las investigaciones en delitos informáticos

Fiscal: Mario Grover Orellana Castillo	**Fiscal: Luis Álvaro Cárdenas Moreno**	**Fiscal: Elías Salcedo Ordaya**
Considera que sí, aunque es un derecho de toda persona el secreto de las comunicaciones, para investigar los delitos informáticos es necesario contar con cierta información que contribuya a la investigación.	Es fundamental contar con esta medida limitativa de derechos, ya que sin ella sería casi imposible identificar al autor del ilícito y careceríamos de pistas sobre quienes están implicados en ellos.	En algunos de ellos
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
En algunos casos sí, especialmente cuando es necesario identificar al titular de la línea telefónica o de cuentas	Considera que es indispensable para las investigaciones en delitos informáticos, ya que, por su naturaleza, se requiere	Considera que, si es importante el levantamiento del secreto de las comunicaciones en las investigaciones de los delitos

electrónicas para llevar a cabo una investigación fiscal.	combatir el uso de medios tecnológicos mediante el levantamiento del secreto de las comunicaciones para obtener datos que ayuden a identificar a los presuntos autores de dichos delitos.	informáticos, para garantizar una tutela efectiva de los bienes jurídicos relacionados con este tipo de delitos. Esto permitirá identificar al titular de la acción u obtener indicios que faciliten la identificación del autor.

Los entrevistados señalan que en algunos casos es importante e indispensable levantar el secreto de las comunicaciones para las investigaciones de delitos informáticos. En general, se requiere identificar al titular de líneas telefónicas, cuentas electrónicas, direcciones IP, entre otros, con la finalidad de facilitar la investigación por parte del fiscal. De lo contrario, no sería posible identificar a los posibles autores y/o partícipes del delito.

Nota: Elaboración propia. Esta tabla se muestra los resultados de la tercera pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas.

Tabla 7

Impacto del requisito de sanción penal en autorización de levantamiento de secreto en casos de fraude informático

Fiscal: Mario Grover Orellana Castillo	**Fiscal: Luis Álvaro Cárdenas Moreno**	**Fiscal: Elías Salcedo Ordaya**
Lo señalado en el artículo 203 se refiere a la intervención y grabación de las comunicaciones, no al levantamiento del	Inicialmente, fue desalentador la no autorización del levantamiento del secreto de las comunicaciones, ya que hace inviable la continuación	En muchos casos, este argumento constituye el fundamento de los jueces para negar el requerimiento solicitado.

secreto de las comunicaciones.	de la investigación. Doy por cierta la argumentación del órgano jurisdiccional en que el delito de fraude informático no supera el extremo mínimo de los cuatro años, por lo tanto, no es accesible la actuación. Sin embargo, la naturaleza de los delitos informáticos cometidos hace imprescindible el levantamiento del secreto de las comunicaciones.	
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
La afectación recae en el Ministerio Público, ya que no logra satisfacer sus expectativas de contar con dicha información, lo cual dificulta sus investigaciones, especialmente debido a la gravedad del asunto, según lo establecido en el artículo 230 del Código Procesal Penal.	Constituye un límite para la investigación por parte del Ministerio Público, ya que no pueden o no disponen de otro medio para identificar a los presuntos autores del delito de fraude informático. La principal limitación es la autorización judicial, para la cual se deben tener en cuenta los criterios y requisitos procesales contenidos en el artículo 230 del Código Procesal Penal.	Efectivamente, constituye un problema en la investigación fiscal en este tipo de delitos debido a las limitadas herramientas disponibles. La principal limitación se presenta al solicitar la autorización a los jueces para realizar el levantamiento del secreto de las comunicaciones. En muchos casos, se obtienen derogatorias por no cumplir con los requisitos establecidos en

	el artículo 230 del Código Procesal Penal, que exige una pena no menor de 4 años de pena privativa. Esto dificulta la investigación para identificar al imputado y puede provocar el archivo del caso.

La negativa en la autorización de intervenciones telefónicas, basada en la falta de cumplimiento de los requisitos procesales establecidos en el artículo 230.1 del Código Procesal Penal, que exige una pena superior a cuatro años para delitos como el fraude informático, representa una limitación significativa. La utilización de estas intervenciones se considera necesaria e imprescindible debido a la naturaleza clandestina de los delitos informáticos y la urgencia de identificar a los posibles autores o cómplices. Sin embargo, esta limitación en nuestra legislación hace inviable la culminación de la investigación.

En relación con lo señalado por el fiscal Mario Grover Orellana Castillo, el Código Procesal Penal utiliza el término "levantamiento del secreto de las comunicaciones" en el párrafo segundo del artículo 230.3.

Nota: Elaboración propia. Esta tabla muestra los resultados de la cuarta pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas.

Tabla 8

Criterios para Aplicar Requisito de Suma Pena en Levantamiento de Secreto de Comunicaciones en Fraude Informático

Fiscal: Mario Grover Orellana Castillo	Fiscal: Luis Álvaro Cárdenas Moreno	Fiscal: Elías Salcedo Ordaya
Al determinar la pena privativa de libertad según lo establecido en la ley 30076 y 30077, modificada en el artículo 45 para la determinación de la pena en tercios, el primer tercio abarca entre 3 años y 4 años 8 meses. Si nos enmarcamos en el tercio inferior, superaría lo señalado en el numeral 1 del artículo 230 del Código Procesal Penal.	En realidad, en los recursos de apelación planteados se ha hecho hincapié en que el artículo 230 no señala que el extremo mínimo deba superar los cuatro años, sino que indica que el delito imputado debe ser superior a cuatro años. En ese sentido, los delitos informáticos tienen penas que van de tres a seis, cuatro a cinco, etc. Lo más importante es reconocer la importancia y la necesidad de contar con esta medida para poder identificar a los autores de estos delitos.	Lo establecido en el Código Penal con la aplicación del sistema de tercios no supera los 4 años, especialmente cuando no existen antecedentes ni circunstancias agravantes.
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
Al entrar al artículo 230 del Código Procesal Penal, he observado que los pocos requerimientos fiscales que he realizado sobre levantamientos del secreto de las comunicaciones han sido denegados debido al tema de la suma de pena,	Los criterios que se toman en cuenta para autorizar el levantamiento del secreto de las comunicaciones son los establecidos en el artículo 230, inciso 1, del Código Procesal Penal. Estos incluyen las necesidades de la medida, la presencia de suficientes	El levantamiento del secreto de las comunicaciones procederá cuando se cumplan los presupuestos de la medida, los cuales deben estar debidamente fundamentados en el requerimiento fiscal,

que es una disposición expresa de la ley procesal penal. Esto se debe a que el delito de fraude informático establece un mínimo de 3 años.	elementos de convicción y que la pena asociada supere los 4 años de pena privativa de libertad. Posteriormente, se tiene en cuenta el test de proporcionalidad.	respaldados con suficientes elementos de convicción. Según la norma antes citada, esta medida procede en las investigaciones de delitos con pena superior a los 4 años y debe superar el principio de proporcionalidad.

Los jueces entrevistados mencionaron que los criterios para aplicar el requisito de una pena superior a los cuatro años en el levantamiento del secreto de las comunicaciones se basan en los requisitos procesales del artículo 230.1 del Código Procesal Penal. Esto implica contar con suficientes elementos de convicción, una pena superior a los cuatro años y la necesidad de la medida, además de cumplir con el test de proporcionalidad en sus tres subprincipios. Sin embargo, en el caso del delito de fraude informático, generalmente no se cumple con el requisito de la pena superior a los cuatro años, ya que está sancionado con una pena mínima de tres años. Esta es la razón por la cual se deniega el requerimiento fiscal en estos casos.

Por otro lado, el criterio de los fiscales para superar el requisito procesal de cuatro años para autorizar la intervención de las comunicaciones es mediante el sistema de tercios.

Nota: Elaboración propia. Esta tabla muestra los resultados de la quinta pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas.

Tabla 9

Impacto del Rechazo de Requerimientos Fiscales por Falta de Suma Pena en Fraude Informático

Fiscal: Mario Grover Orellana Castillo	**Fiscal: Luis Álvaro Cárdenas Moreno**	**Fiscal: Elías Salcedo Ordaya**
Hasta el momento, no se ha encontrado inconveniente, ya que normalmente estos delitos se cometen en banda y/u organización criminal, o en concurso con otros delitos, lo que implica que las penas privativas de libertad se suman.	Inicialmente sí, pero a través de la necesidad impugnatoria hemos logrado cambiar el criterio que tienen los jueces respecto a este delito y su utilidad para el éxito de la investigación.	Sí, se archivan los casos
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
Los señores fiscales no han apelado las denegatorias de sus requerimientos, lo cual entiendo ha dificultado sus investigaciones en casos de fraude informático.	Los representantes del Ministerio Público, en casos de delitos informáticos en los que se requiere el levantamiento del secreto de las comunicaciones, han experimentado rechazos y no apelaron. Entendemos que esto lleva al archivo de los casos, ya que no lograron obtener elementos de convicción que respalden su caso.	Durante su experiencia, no se ha requerido por parte del Ministerio Público el levantamiento del secreto de las comunicaciones en casos de delitos de fraude. Además, cabe destacar que han sido muy pocas las investigaciones por este tipo de delitos.

Los jueces entrevistados señalaron que los criterios utilizados se toman en cuenta desde los requisitos procesales contenidos en el artículo 230.1 del Código Procesal Penal. Estos incluyen suficientes elementos de convicción, pena superior a los cuatro años y la necesidad de la medida. Asimismo, se debe superar el test de proporcionalidad en sus tres subprincipios. Sin embargo, en el delito de fraude informático, generalmente no cumple con el requisito procesal de la pena superior a los cuatro años, ya que está sancionado en su extremo mínimo con una pena de tres años. Esta es la razón por la cual se niega el requerimiento fiscal en estos casos.

El criterio de los fiscales difiere en cuanto a la forma de superar el requisito procesal de cuatro años para autorizar la intervención de las comunicaciones es el sistema de tercios.

Nota: Elaboración propia. Esta tabla se muestra los resultados de la sexta pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas.

Tabla 10

Impacto de la restricción por la pena mínima en la identificación y persecución de responsables del fraude informático

Fiscal: Mario Grover Orellana Castillo	**Fiscal: Luis Álvaro Cárdenas Moreno**	**Fiscal: Elías Salcedo Ordaya**
Considera que no, como se ha señalado anteriormente, para el levantamiento del secreto de las comunicaciones no	Por supuesto que sí, por ello considero que dicho artículo debe ser modificado en cuanto a este tipo de delitos,	Sí afecta

es necesario que la pena privativa de libertad sea superior a los 4 años.	específicamente el fraude informático.	
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
Considera que sí, por lo que debería revisarse a fondo legislativamente.	Considera que el límite impuesto por el Código Procesal Penal, como requisito procesal, afecta la identificación y persecución del delito de fraude informático. La imposibilidad de identificar a los posibles actores crea impunidad ante este tipo de delitos.	Teniendo en cuenta que este tipo de delitos en el mundo contemporáneo tienden a incrementarse, es necesario conceder el levantamiento del secreto de las comunicaciones para evitar que queden impunes los delitos de fraude informático. Esto permitiría que el fiscal recabe los elementos de convicción necesarios para acreditar el ilícito penal, siempre respetando los límites establecidos por las normas.

Según los jueces entrevistados, la investigación se ve obstaculizada, lo que dificulta la identificación de autores y cómplices, así como la persecución del delito de fraude informático. Para evitar la impunidad, consideran crucial autorizar la intervención de las comunicaciones y sugieren una revisión legislativa en este aspecto para una eventual reforma.

En cuanto al criterio de los fiscales, resaltan que el requisito de una pena superior a cuatro años representa una limitación significativa, enfatizando la necesidad de recurrir al sistema de tercios para superar esta barrera.

Nota: Elaboración propia. Esta tabla muestra los resultados de la séptima pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas.

Tabla 11

Sobre la autorización judicial del levantamiento de secreto de las comunicaciones en delitos informáticos: ¿Se debe tener en cuenta la Ley 27697, solo el numeral 1 del artículo 230 o ambos?

Fiscal: Mario Grover Orellana Castillo	**Fiscal: Luis Álvaro Cárdenas Moreno**	**Fiscal: Elías Salcedo Ordaya**
Considera que sí, ya que afectar un derecho constitucional debe realizarse con todos los requisitos, incluyendo una doble motivación o una motivación reforzada.	Actualmente, lo que se utiliza es lo establecido en el artículo 230 del NCPP, que resulta suficiente para solicitar al juez de garantías el levantamiento del secreto de las comunicaciones.	Ya no, ya que el juez utiliza el NCPP.
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
Dicha ley ahora sí contempla la expedición para delitos informáticos, conforme al numeral adicionado por la tercera disposición	Dicha ley otorga una facultad en la que se excluye uno o más requisitos del Código Procesal Penal; sin embargo, se debería	En primer lugar, debemos tener presente las jerarquías de las normas, teniendo por un lado el artículo 230, inciso 1, del Código Procesal Penal y, por otro lado, la ley número

complementaria modificatoria de la ley N°30963, por lo que podría aplicarse.	aplicar el criterio del principio de especialidad.	27697. En este contexto, debe prevalecer el Código Procesal Penal; sin embargo, se puede conceder autorización para el levantamiento del secreto de las comunicaciones de manera excepcional, siempre y cuando el fiscal lo solicite mediante un requerimiento debidamente motivado, acompañado de suficientes elementos de convicción.

La Ley 27697 establece una excepción para la autorización judicial en la interceptación de las comunicaciones relacionadas con los delitos informáticos, y esta normativa puede aplicarse en conjunto con el CPP bajo el principio de especialidad. Actualmente, se siguen los criterios establecidos en el artículo 230.1 del CPP para obtener la autorización judicial en la intervención de las comunicaciones y telecomunicaciones.

Nota: Elaboración propia. Esta tabla muestra los resultados de la octava pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas.

Tabla 12

Perspectiva sobre el equilibrio entre derechos fundamentales y necesidades de investigación en fraude informático

Fiscal: Mario Grover Orellana Castillo	**Fiscal: Luis Álvaro Cárdenas Moreno**	**Fiscal: Elías Salcedo Ordaya**
Considera que, al ponderar la lesión de los derechos	Desde la perspectiva de la ponderación de la	Se debe aplicar el test de proporcionalidad

fundamentales, estaría justificado en aras de la necesidad de buscar la verdad a través de la investigación y esclarecer adecuadamente el delito de fraude informático, que es uno de los derechos fundamentales.	proporcionalidad de las medidas limitativas de derechos, considero que el levantamiento del secreto de las comunicaciones en una investigación de delitos informáticos es completamente necesario para salvaguardar los fines del proceso, como el esclarecimiento de los hechos y la obtención de los medios de prueba. Es la única herramienta que puede concretar este objetivo, ya que permite identificar a los autores y partícipes del injusto penal. En relación con la necesidad, no hay otra medida que pueda otorgar el mismo resultado, por lo que resulta proporcional.	
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
Aplicar el principio de proporcionalidad, a través de su componente conocido como "principio de proporcionalidad en	Es necesario equilibrar o ponderar la lesión con el objetivo de la restricción del derecho. En otras palabras, no podemos sacrificar un	La ponderación se realiza en momentos de expedir la resolución de autorización de levantamiento del secreto de las comunicaciones. Esto

sentido estricto", consiste en aplicar la ley de ponderación basándose en que cuanto mayor sea el grado de la no satisfacción o afectación de un principio, tanto mayor tiene que ser la importancia de la satisfacción del otro.	derecho fundamental como el secreto a las comunicaciones si no existe la extrema necesidad de requerirlo en una investigación.	se debe a que se deben cumplir con los requisitos para su concesión, entre los cuales se encuentra el principio de proporcionalidad de la medida. Este principio se subdivide en tres principios: idoneidad, necesidad y proporcionalidad en sentido estricto. En tal sentido, se debe ponderar el derecho que tiene el imputado y el bien jurídico protegido.

Los criterios para autorizar la medida restrictiva del derecho al secreto e inviolabilidad de las comunicaciones, además de considerar los requisitos procesales establecidos en la normativa, deben evaluarse mediante el test de proporcionalidad, aplicando sus tres subprincipios (idoneidad, necesidad y proporcionalidad en sentido estricto). Esto implica sopesar la afectación al derecho fundamental del secreto e inviolabilidad de las comunicaciones frente a la necesidad de la medida, la cual será útil en la búsqueda de la verdad.

La restricción al derecho fundamental del secreto e inviolabilidad de las comunicaciones se justifica por la necesidad de la medida en pro de la investigación para esclarecer los hechos mediante la obtención de medios de prueba. En los delitos informáticos, especialmente en el fraude informático, la intervención de las comunicaciones se presenta como la única herramienta viable para lograr este objetivo en la mayoría de los casos.

Nota: Elaboración propia. Esta tabla muestra los resultados de la novena pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas.

Tabla 13

Evaluación sobre el grado de lesividad de la medida de levantamiento del secreto de las comunicaciones en investigaciones de fraude informático

Fiscal: Mario Grover Orellana Castillo	**Fiscal: Luis Álvaro Cárdenas Moreno**	**Fiscal: Elías Salcedo Ordaya**
Ningún derecho es absoluto; todos los derechos son relativos. Considero que debe primar el derecho a la búsqueda de la verdad dentro de la teoría de la ponderación. Según Robert Alexy, todos los principios son desarrollables, y en este caso, se debería dar prioridad a los derechos de la colectividad frente al derecho individual de las personas.	Partiendo del hecho de que en este tipo de delitos los bienes jurídicos protegidos son de diversa naturaleza, como el patrimonio, intimidad, propiedad intelectual, fe pública, entre otros, el delito de fraude informático se dirige hacia el patrimonio, que también es un derecho fundamental contenido en la propiedad y que ha sido vulnerado por el sujeto activo del delito. En este sentido, al haber una ponderación entre el injusto cometido y la intervención en el derecho del investigado, considero que debe darse mayor preeminencia y	No existe afectación a los intereses del Estado con la lesividad de la medida restrictiva. El Estado debe ser transparente en todos sus actos.

	ponderación al fin supremo de la justicia.	
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
La lesividad está presente en cualquier caso en el que se disponga el levantamiento del secreto de las comunicaciones.	La ponderación general entre los intereses del Estado y los derechos fundamentales de las personas a las que se les intervienen las comunicaciones y las telecomunicaciones está sujeta al test de proporcionalidad. De esta manera, se evalúa si en la investigación es realmente necesario levantar el secreto de las comunicaciones para esclarecer los hechos. En este sentido, se debe considerar el beneficio de la intervención de las comunicaciones y asegurar que la lesión del derecho fundamental sea proporcional a dicho beneficio.	En primer lugar, debemos precisar que el principio de lesividad implica la exclusiva protección de bienes jurídicos, manifestándose como un principio de ofensividad y como la expresión de una efectiva puesta en peligro de un bien jurídico. En este contexto, corresponde realizar una ponderación para determinar si el derecho constitucional al secreto de las comunicaciones, que goza toda persona, resulta necesario o no para proteger dicho bien jurídico. En el caso particular, para que proceda el levantamiento del secreto de las comunicaciones, la investigación debe ser compleja y, por tanto, la intervención debe ser considerada imprescindible.

La lesividad se manifiesta cada vez que se considera restringir el derecho al secreto de las comunicaciones. Por lo tanto, es crucial evaluar el beneficio de la intervención en las comunicaciones frente al daño al derecho fundamental, utilizando el test de proporcionalidad.

El fraude informático, al ser un delito que afecta el derecho fundamental al patrimonio, justifica la intervención en las comunicaciones como una medida restrictiva necesaria para descubrir la verdad. En este contexto, es esencial sopesar la necesidad de investigar el delito y la restricción del derecho fundamental. Se debe dar mayor importancia y consideración al fin supremo de la justicia.

Nota: Elaboración propia. Esta tabla muestra los resultados de la décima pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas.

Tabla 14

Grados de Lesión en la Restricción a Derechos Fundamentales

Fiscal: Mario Grover Orellana Castillo	**Fiscal: Luis Álvaro Cárdenas Moreno**	**Fiscal: Elías Salcedo Ordaya**
No, ya que solo se afecta el derecho a la intimidad.	Es indudable que existen grados de afectación en cuanto al tipo de intervención de las comunicaciones. Un ejemplo es que la información histórica es menos invasiva a la intimidad y al secreto de las	No, porque si es necesario, debe levantarse el secreto.

	comunicaciones en comparación con la interceptación en tiempo real. Por tanto, el tipo de lesión a estos derechos fundamentales tendrá su correspondencia con el tipo de delito investigado. Entre mayor sea la lesión, mayor tendrá que ser la justificación y necesidad para realizarlas.	
Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
Considera que la afectación es única y no puede diferenciarse en grados, es decir, no puede medirse.	Considera que sí existen diferentes grados de lesión a los derechos fundamentales en casos que involucran información histórica, interceptación en tiempo real y geolocalización. La interceptación en tiempo real, por ejemplo, implica una mayor lesión al derecho restringido al permitir escuchar conversaciones privadas entre personas. En contraste, en los casos de	Considera que sí existen diferentes grados de lesión a los derechos fundamentales, por lo que se debe aplicar un enfoque basado en los principios de razonabilidad y proporcionalidad al evaluar la necesidad de la medida restrictiva del secreto de las comunicaciones. Es esencial realizar una ponderación entre el derecho afectado y la finalidad de la investigación. La intervención de las comunicaciones debería ser ordenada solo cuando sea el

	obtención de información histórica, la lesión es menor, ya que esta medida es menos intrusiva.	único medio para esclarecer los hechos, especialmente en investigaciones con pluralidad de agentes u otros elementos de convicción insuficientes para acreditar los hechos. En consecuencia, no en todos los casos se justifica esta medida, en situaciones específicas.

Existe controversia entre las respuestas de los entrevistados, ya que algunos reconocen la existencia de grados de afectación en las intervenciones telefónicas. Consideran que, al autorizar judicialmente dichas intervenciones, es fundamental aplicar los principios de razonabilidad y proporcionalidad de la medida.

Argumentan que la interceptación en tiempo real es más intrusiva con respecto al derecho a la intimidad y al secreto de las comunicaciones en comparación con la obtención de información histórica, que resulta menos invasiva. Sin embargo, otros entrevistados no comparten esta perspectiva y sostienen que no existen diferencias ni grados de lesión en la intervención de las comunicaciones.

Nota: Elaboración propia. Esta tabla muestra los resultados de la undécima pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas.

Tabla 15

Diferencias en criterios para levantamiento de secreto de comunicaciones en tiempo real, geolocalización e información histórica

Fiscal: Mario Grover Orellana Castillo	Fiscal: Luis Álvaro Cárdenas Moreno	Fiscal: Elías Salcedo Ordaya
Hasta el momento, el criterio utilizado por el juez es el mismo, señalando y argumentando siempre sobre el derecho constitucional a la intimidad y la viabilidad de las comunicaciones.	En cuanto a nuestra legislación, el criterio utilizado para resolver ese tipo de pedidos está regulado en el artículo 230, inciso 1, del Código Penal. Sin embargo, considero que los señores jueces efectúan una interpretación errónea al señalar que constituye una exigencia que sirve para declarar fundado este pedido, argumentando que se trata de delitos con penas superiores a cuatro años. En su extremo mínimo, cuando la norma no los exige textualmente así. Por otro lado, desde mi experiencia en la recopilación de información y la adquisición de pruebas electrónicas de proveedores de Estados Unidos, la relación al nivel de privacidad que otorga la ley al suscriptor indica que, cuanto más nos adentremos en la privacidad del individuo, mayor será la carga legal del	Que no, cuando estamos ante un delito flagrantes es necesario, pero cuando no existe está causal si se vulnera derechos fundamentales.

	requirente, en este caso, del Ministerio Público.	

Juez: Rafael Agustín Herrera Rivas	**Juez: Michael Henry Rojas Chancasanampa**	**Juez: Segundo Juan Huamán Carrasco**
Hasta hace poco, se mantenía el mismo criterio de negar el requerimiento cuando no cumplía con el requisito de la suma de penas. Sin embargo, este enfoque ha venido variando, dependiendo del caso concreto y de conformidad con la Ley 27697.	En su experiencia, no existe diferencia en los criterios utilizados para resolver la autorización del levantamiento del secreto de las comunicaciones en tiempo real, geolocalización o información histórica. La legislación establece los requisitos para su autorización y no distingue entre ellas, a pesar de que en la práctica se evidencia la necesidad de hacerlo. Por lo tanto, el criterio utilizado en estos casos es el mismo.	Para conceder la intervención de las comunicaciones, se tienen en cuenta los mismos criterios, ambos relacionados con derechos fundamentales reconocidos en la Constitución Política del Estado. Mayormente, el fiscal, al solicitarlo, también pide la interceptación de las comunicaciones en tiempo real, geolocalización e información histórica, claro está, en relación con otros delitos cuyas penas superan los cuatro años.

El criterio es unánime para resolver la intervención de las comunicaciones, dado que los artículos 230 y 231 del Código Procesal Penal no establecen diferencias en los requisitos para autorizar la intervención en sus distintas formas, ya sea interceptación en tiempo real, geolocalización o acceso a información histórica.

Nota: Elaboración propia. Esta tabla muestra los resultados de la duodécima pregunta de la entrevista realizada a jueces y fiscales, así como un breve resumen de las respuestas.

4.2. Análisis y discusión de resultados

El objetivo general de la investigación fue examinar cómo el requisito de *suma pena* según lo estipulado en el numeral 1 del artículo 230 del Código Procesal Penal, para la autorización judicial del levantamiento del secreto de las comunicaciones en forma de información histórica, afecta la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo durante el periodo 2021 y 2022.

En la investigación se recopilaron datos relevantes mediante entrevistas con jueces de investigación preparatoria y fiscales, los cuales proporcionaron sus criterios sobre la intervención de las comunicaciones. Estas respuestas reflejan los criterios adoptados por ellos al requerir esta medida restrictiva y al autorizarla.

Se ha determinado a través de las respuestas que la mayoría de los jueces y fiscales están de acuerdo en que la negación de la autorización judicial para la intervención de las comunicaciones afecta significativamente el desarrollo de las investigaciones. En muchas ocasiones, esto conduce al archivo o sobreseimiento de los casos al no contar con los elementos de convicción que solo pueden obtenerse mediante la intervención de las comunicaciones, una medida especialmente necesaria en los delitos informáticos que utilizan tecnología para cometer delitos y afectar bienes jurídicos protegidos.

Esto contrasta con la experiencia vivida en 2022, durante mi participación en el Servicio Civil de Graduandos (SECIGRA) en la CSJJU en los JIP, donde surgió el problema de la limitación del requisito de una pena superior a cuatro años para autorizar la

intervención de las comunicaciones en delitos informáticos, especialmente en casos de fraude informático. Bajo la interpretación de los jueces, la pena considerada es el mínimo del delito investigado para superar el requisito procesal de los cuatro años.

Las penas establecidas en la Ley de Delitos Informáticos (Ley 30096) generalmente no superan el mínimo de cuatro años de pena. El delito de fraude informático, que es el delito informático más común según el artículo 8 de esta ley, prevé una pena de tres a ocho años, lo cual, según esta interpretación, no cumple con el requisito y dificulta la autorización e incluso el pronunciamiento sobre el fondo del asunto.

En comparación con la legislación extranjera, en España se diferencian los tipos de levantamiento del secreto de las comunicaciones según sus requisitos y principios aplicables, determinando diferencias según la gravedad de la lesión al derecho fundamental. La legislación argentina difiere de la peruana en el sentido de que el fiscal puede intervenir en las comunicaciones equivalentes a la obtención de información histórica sin autorización judicial en casos de *periculum in mora*, aunque debe ser convalidada por el juez. Por otro lado, la legislación colombiana permite la intervención de las comunicaciones a discreción del fiscal, sin control judicial, lo cual ha suscitado preocupación por su posible uso arbitrario.

Por ello, considero que la regulación adecuada de las medidas restrictivas, como el derecho al secreto de las comunicaciones, debe sostenerse en una especie de balanza, permitiendo al fiscal actuar cuando sea realmente necesario y razonable, sustentado en elementos de convicción que describan la necesidad y finalidad de la medida.

Investigaciones a nivel nacional han demostrado la necesidad de estas medidas en delitos informáticos, como lo señalan estudios realizados por Lunarejo y Rodríguez (2021)

y Coronado y Segura (2018), que destacan la importancia de obtener datos que solo pueden conseguirse mediante el levantamiento del secreto de las comunicaciones para avanzar en las investigaciones.

Así se evidencia la necesidad de utilizar la intervención de las comunicaciones en casos de fraude informático, principalmente para identificar a los autores y partícipes de los delitos, así como para obtener información relevante que sea útil durante la investigación y en la etapa de juzgamiento.

En este contexto, se puede deducir que para investigar el delito de fraude informático es necesario recopilar datos históricos que solo pueden obtenerse mediante la intervención de las comunicaciones, con el propósito principal de identificar a los responsables del acto criminal. A través de esta intervención, se pueden obtener datos generales y registros de comunicación escrita, como mensajes de texto o correos electrónicos, entre otros. El fiscal requiere principalmente esta información histórica y datos generales de los titulares de las comunicaciones para lograr los objetivos de la medida, sin necesidad de acceder al contenido específico de las comunicaciones.

Es importante señalar que los entrevistados solo consideran las disposiciones legales establecidas en el CPP al solicitar y decidir sobre la autorización para la intervención de las comunicaciones, siguiendo lo establecido en el protocolo de actuación conjunta, y dejando de lado la Ley 27697 a pesar de que aún está en vigencia.

En este contexto, con los datos obtenidos de la muestra se ha determinado que el incumplimiento del requisito de una pena superior a cuatro años de privación de libertad en el extremo mínimo del delito de fraude informático impide la autorización para la intervención de las comunicaciones. Esta situación afecta gravemente la investigación del

delito de fraude informático, lo que finalmente conduce a su archivo o sobreseimiento, generando impunidad para los autores y partícipes del delito.

El primer objetivo específico busca determinar en qué medida el requisito de suma pena restringe los requerimientos fiscales de levantamiento del secreto de las comunicaciones en la investigación de delitos de fraude informático en los juzgados de Huancayo durante el periodo 2021 y 2022.

De las entrevistas realizadas se determinó que este requisito procesal impide la autorización de la intervención de las comunicaciones. Los jueces entrevistados interpretan este requisito como la pena mínima del delito investigado, mientras que los fiscales consideran necesario utilizar el sistema de tercios para superar este requisito.

La CSJR ha indicado que el sistema de tercios se utiliza una vez que se han evaluado los hechos probados, determinado la culpabilidad del imputado y realizado una precisión cualitativa y cuantitativa para determinar la pena (Casación N° 723-2018 Junín). Asimismo, sostuvo que la determinación de la pena implica concretar la sanción penal mediante el uso del sistema de tercios, considerando el injusto, la culpabilidad del hecho y el principio de proporcionalidad (Casación N° 68-2019 Lambayeque).

Por lo tanto, la aplicación del sistema de tercios para determinar la pena debe reservarse para la etapa final del juzgamiento, cuando se haya establecido con precisión la culpabilidad del acusado (Prado, 2018).

La intervención de las comunicaciones tiene como finalidad la obtención de medios probatorios, siendo la etapa de investigación preparatoria el momento adecuado para llevarla a cabo. Se deja abierta la posibilidad de autorizarla en diligencias preliminares

cuando aún no se ha determinado con exactitud el delito investigado. En este sentido, desnaturalizaría el sistema de tercios y sería incongruente utilizarlo para superar el requisito de la pena mínima necesaria para autorizar intervenciones telefónicas.

La interpretación del requisito de una pena superior a cuatro años para autorizar la intervención de las comunicaciones en el extremo mínimo del delito investigado sería el criterio más adecuado al tratarse de una medida restrictiva del derecho fundamental al secreto de las comunicaciones. Esto se sustenta en el principio de *in dubio pro-reo* (artículo 139.11 de la Constitución), que establece que la norma debe interpretarse de manera favorable al acusado en caso de duda o contradicción normativa. Este principio refuerza el argumento de que el sistema de tercios no es aplicable en la etapa de investigación preparatoria, ya que está diseñado para la etapa de juzgamiento, una vez determinada la culpabilidad del acusado.

Destacamos que ni los jueces ni los fiscales consideran la Ley 27697, la cual faculta a los fiscales para intervenir las comunicaciones, y otorga a los jueces la facultad de conocer y controlar dicha intervención. Esta ley enumera en su artículo 1 un catálogo de 16 delitos, incluyendo los delitos informáticos, sin establecer requisitos procesales ni formales. Por lo tanto, se entiende que esta ley se rige exclusivamente por el principio de proporcionalidad y sus subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto. Esto deja de lado los requisitos procesales establecidos en el artículo 230 del CPP. Los criterios descritos en el protocolo de actuación conjunta, aprobado por el Ministerio Público y el Poder Judicial, indican que los artículos 230 y 231 del CPP regirán en los distritos judiciales donde el CPP esté vigente, mientras que la Ley 27697 será aplicable en los distritos judiciales donde el C. de PP aún esté vigente.

En este sentido, señalamos que la Ley 27697 sigue vigente, ya que una ley solo puede ser derogada por otra ley o declarada inconstitucional por el Tribunal Constitucional, según lo establecido en los artículos 103 y 204 de la Constitución. Por lo tanto, esta ley especial aún está en vigor, aunque esté desactualizada; sin embargo, los entrevistados consideran únicamente la aplicación del CPP, ignorando la ley especial.

Bajo estos criterios, el requisito de una pena mínima establecido en el artículo 230.1 del CPP restringe significativamente la viabilidad de las solicitudes de autorización para la intervención de comunicaciones en forma de información histórica, sin considerar que, dada la naturaleza del delito de fraude informático, se requieren técnicas especiales de investigación para poder identificar principalmente a los autores del delito.

El segundo objetivo específico busca determinar el grado de lesividad de la medida restrictiva de derechos de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo durante el periodo 2021-2022.

Se ha evidenciado que existen dos criterios diferidos entre los entrevistados sobre los grados de lesividad en la intervención de las comunicaciones. Estos son: (a) la afectación del derecho por la intervención de las comunicaciones es única y no puede medirse en grados; y, (b) los grados de afectación en cuanto al tipo de intervención de las comunicaciones, pues la información histórica es menos invasiva al secreto e inviolabilidad de las comunicaciones, a diferencia de la interceptación de las comunicaciones en tiempo real, que es más intrusiva.

Es cierto que nuestra legislación no diferencia conceptualmente los diferentes tipos de intervención de las comunicaciones ni la finalidad de cada una de estas. Nos valemos

de otras fuentes del derecho, como la doctrina y jurisprudencia; sin embargo, este tema está poco desarrollado. Por ello, cobra importancia el protocolo de actuación conjunta para comprender su finalidad. Se evidencia así la necesidad de diferenciar a nivel conceptual y establecer requisitos procesales razonables y diferenciados en la intervención de las comunicaciones, ya sea histórica, de geolocalización o escuchas telefónicas en tiempo real, de acuerdo con el grado de lesión que puedan causar al derecho fundamental.

La CSJR señaló que el registro de llamadas, del que se recaba información sobre el proceso de comunicación sin acceder al contenido de esta, conocido como técnica de recuento, que engloba la frecuencia de llamadas, duración e identidad de los interlocutores, es menos invasivo (Expediente N° 04-2018-31). Asimismo, el derecho al secreto de las comunicaciones protege el contenido de las comunicaciones, su soporte y las circunstancias que la rodean. Los listados de llamadas son menos intrusivos que la interceptación en tiempo real de la comunicación, por lo que la autorización judicial debe ser de menor rigor (Recurso de apelación N° 04-2015 "3"). Estos criterios fueron adoptados por influencia del TEDH, que señaló que la entrega de listados de llamadas por las compañías telefónicas es menos intrusiva que las escuchas telefónicas, permitiendo que la autorización judicial sea excepcional (Caso Malone contra el Reino Unido, 1984).

Legislativamente, aunque no se desarrollen conceptualmente los niveles de intervención de las comunicaciones, esto debe ser desarrollado en los requerimientos fiscales y principalmente en la autorización judicial. Se determina el grado de lesividad al valorar la intrusión y afectación al derecho del secreto de las comunicaciones y la intimidad personal, con la finalidad de la investigación y lo que pueda obtenerse de esta medida

restrictiva de derechos. El sacrificio de este derecho fundamental debe dar como resultado un beneficio proporcional en la investigación.

De las respuestas obtenidas de los cuestionarios, se observa que para el delito de fraude informático se requieren principalmente datos para identificar a los posibles autores y partícipes del delito. En este sentido, con la intervención de las comunicaciones solo se requieren datos históricos, sin acceder al contenido de las comunicaciones.

Los magistrados, en aplicación del principio de discrecionalidad, deben diferenciar en la intervención de las comunicaciones, además de sus tipos (histórica, de geolocalización e interceptación), si estas afectan al contenido de la comunicación o solo a su instrumento o soporte. Estos criterios deben adoptarse para determinar si esta medida es más o menos intrusiva al restringir este derecho fundamental, con respecto al beneficio que se obtendrá con la ejecución de la medida.

Es indispensable señalar los grados de lesividad en la intervención de las comunicaciones en su tipo de información histórica e interceptación en tiempo real, tomando en cuenta si se afecta el contenido propio de la comunicación o solo su instrumento y soporte. Además, la información histórica no solo afecta al instrumento de las comunicaciones, sino también a su contenido, mediante la apertura de mensajes de texto, correos electrónicos, mensajes en redes sociales, etc.

Figura 5

Niveles de lesividad según tipo de intervención de las comunicaciones

Nota: Elaboracion propia, la figura detalla los grados de lesividad en la intervencion de las comunicaciones en sus tipos de informacion historica e interceptacion.

En este sentido, el grado de lesividad de la intervención de las comunicaciones en su tipo de información histórica es menos gravoso e intrusivo en comparación con la interceptación de las comunicaciones, incluso si se abrieran y conocieran mensajes que lesionen el contenido de la comunicación, ya que estos son históricos y tanto el remitente como el destinatario conocen el riesgo en el que cualquiera de ellos puede utilizar esa información escrita e incluso hacerla pública.

En conclusión, por su naturaleza, la investigación del delito de fraude informático requiere de medios especiales para identificar a los autores y partícipes del delito, lo cual solo se logra mediante la intervención de las comunicaciones. Por ello, se debe considerar su autorización, ya que la lesión al derecho fundamental es mínima en la información histórica en relación con la necesidad de la medida en los delitos de fraude informático, pues resultan ser idóneas.

CONCLUSIONES

1. La aplicación del requisito de *suma pena* establecido en el artículo 230, numeral 1 del CPP para levantar el secreto de las comunicaciones limita seriamente la investigación del delito de fraude informático a cargo del fiscal. Los juzgados de investigación preparatoria de Huancayo suelen declarar la improcedencia liminar de los requerimientos fiscales, lo que imposibilita identificar a los autores y/o partícipes del delito, así como obtener elementos de convicción relevantes para verificar las circunstancias del ilícito penal, lo que lleva al archivo preliminar o sobreseimiento del caso.

2. El levantamiento del secreto de las comunicaciones en su forma de información histórica, a pesar de su mínimo grado de lesividad o afectación al derecho fundamental de los investigados por fraude informático, restringe totalmente la posibilidad de autorizar judicialmente la medida. Esto se debe a que no cumple con la exigencia de una sanción penal conminada superior a cuatro años de pena privativa de libertad en su extremo mínimo, lo que impide al fiscal obtener elementos de convicción para identificar a los autores y/o partícipes del delito.

3. Nuestra legislación procesal, tanto general como especial, no diferencia requisitos procesales para la autorización judicial en la forma de intervención de las comunicaciones, ya sea histórica, de geolocalización o interceptación en tiempo real. Tampoco considera el grado de intrusión o lesión al derecho fundamental al secreto de las comunicaciones reconocido constitucionalmente. A pesar de que la intervención histórica es menos intrusiva y lesiva en comparación con la interceptación en tiempo real, su tratamiento respecto a los requisitos procesales debe diferenciarse.

RECOMENDACIONES

1. Se debe promover un tratamiento normativo adecuado con respecto a la intervención de las comunicaciones en su modalidad de información histórica para investigar el delito de fraude informático. Esto debe tener en cuenta la naturaleza específica de este delito, la necesidad de emplear técnicas especiales de investigación y el grado de afectación e intrusión en el derecho fundamental. Se recomienda modificar el artículo 230.1 del Código Procesal Penal y la Ley 27697 en este sentido.

2. Los jueces de garantía y fiscales encargados de los casos de delitos informáticos deben establecer espacios de diálogo académico. En estos espacios, se debe discutir la deficiencia normativa del artículo 230.1 del Código Procesal Penal en relación con el requisito de suma pena que limita la investigación fiscal. Asimismo, se debe abordar la aplicación de la Ley 27697 para establecer límites procesales adecuados que eviten su uso abusivo y arbitrario. Finalmente, es necesario cuestionar las disposiciones del protocolo de actuación conjunta respecto al uso de ambos cuerpos normativos.

3. Se recomienda promover criterios normativos que diferencien la intervención de las comunicaciones según sus niveles de afectación, considerando los tipos de intervención: histórica, de geolocalización e interceptación en tiempo real. Estos criterios deben diferenciar los requisitos procesales teniendo en cuenta el grado de lesión al derecho fundamental afectado y la naturaleza particular de ciertos delitos, como los delitos informáticos (ciberdelitos).

REFERENCIAS BIBLIOGRÁFICAS

Abad, S. (2012). El derecho al secreto de las comunicaciones. *Alcances, límites y desarrollo jurisprudencial. Pensamiento Constitucional, 16*(16), 12-29. https://revistas.pucp.edu.pe/index.php/pensamientoconstitucional/article/view/2852/2780

Acurio, S. (2016). *Delitos informáticos: Generalidades.* https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Alexy, R. (2000). La institucionalización de los derechos humanos en el estado constitucional democrático. *Derechos y Libertades: revista del Instituto Bartolomé de las Casas, 5*(8), 21-41. https://hdl.handle.net/10016/1372

Arbulu, V. (2015). *Derecho Procesal Penal.* Gaceta Jurídica.

Bernal, C. (2003). *El principio de proporcionalidad y los derechos fundamentales.* Centro de estudios políticos y constitucionales.

Blancas, G. (2012). Medidas a seguir para el levantamiento del secreto de las comunicaciones y telecomunicaciones (arts 230 y 231 del NCCP). *Horizonte Empresarial*(10), 63-72. https://doi.org/10.31381/horizonte_empresarial.v0i10.248

Bustamante, R. (2001). *El derecho a probar como elemento esencial en un proceso justo.* Ara Editores.

Carbone, C. (2005). *Grabaciones, escuchas telefónicas y filmaciones como medios de prueba.* Rubinzal-Culzoni.

Carbone, C. (2008). *Requisitos constitucionales de las intervenciones telefónicas.* Rubinzal-Culzoni.

Casación N° 342 - 2011 Cusco, 342 (Corte Suprema 2011).

Casación N° 68-2019 Lambayeque, 68 (Corte Suprema 2019).

Casación N° 723-2018 Junín, 723 (Sala Penal Transitoria).

Casanova, R. (2014). *Las intervenciones telefónicas en el proceso penal.* Bosch.

Caso Malone contra el Reino Unido, 8691/79 (Tribunal Europeo de Derechos Humanos 2 de Agosto de 1984).

Castillo, J. (2022). ¿La información probatoria obtenida en el levantamiento del secreto de las comunicaciones se puede utilizar en otro proceso y/o procedimiento distinto al penal? *Gaceta Penal y Procesal Penal,* (159), 9-35.

Castillo, J. (2022). Notas sobre el contenido esencial del artículo 2.10 de la Constitución sobre el derecho a la inviolabilidad de las comunicaciones en el proceso penal. *Gaceta Penal y Procesal Penal,* (158), 265-272.

Coronado, R. y Segura, L. (2018). *La actuación del representante del Ministerio Público frente al levantamiento del secreto de las comunicaciones [Tesis de grado].* Universidad Señor de Sipán. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/6051/Coronado%20Tarrillo%20%26%20Segura%20Samillan.pdf?sequence=1&isAllowed=y

Croda, J. y Abad, E. (2016). Modelos de investigación cualitativa y cuantitativa y su aplicación en el estudio del derecho. *Revista electrónica de investigación de la Universidad de Xalapa,* (4), 12.

De Langhe, M. (2009). *Escuchas telefónicas. Límites a la intervención del Estado en la privacidad e intimidad de las personas.* Hammurabi.

Defensoría del Pueblo. (2023). *La ciberdelincuencia en el Perú: Estrategias y retos del estado.* Depósito Legal en la Biblioteca Nacional del Perú N° 2023-03511.

https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Díaz, F. (2006). El derecho fundamental al secreto de las comunicaciones. *Derecho PUCP: Revista de la Facultad de Derecho*, (59), 159-175. https://doi.org/10.18800/derechopucp.200601.007

El Peruano. 22 de junio de 2023. *Cuidado con los fraudes informáticos. Estas son las modalidades más denunciadas en Perú.* https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru

Escher y otros vs. Brasil (Corte Interamericana de Derechos Humanos 6 de Julio de 2009).

Escudero, C. y Cortez, L. (2018). *Técnicas y métodos cualitativos para la investigación científica.* Editorial UTMACH.

Expediente. N° 018-2003-AI/TC (Tribunal Constitucional, 2004).

Expediente. N° 00867-2011-PA/TC (Tribunal Constitucional, 2014).

Expediente. N° 579-2008-PA/TC (Tribunal Constitucional, 2008).

Expediente. N° 01470-2016-PHC/TC (Tribunal Constitucional, 2019).

Expediente N° 04-2018-31 (Sala Penal Especial).

Farfán, F. (2007). *La interceptación de las comunicaciones en el proceso penal y disciplinario.* Procuraduría General de la Nación. https://doi.org/https://www.ejercito.mil.co/enio/recurso_user/doc_contenido_pagina_web/800130633_4/613544/17._libro.pdf

Feijóo, R. (2021). Hacia una adecuada protección del derecho fundamental al secreto e inviolabilidad de las comunicaciones en la relación laboral: Análisis constitucional

a la luz de nuevas tecnologías. *THEMIS Revista de Derecho,* (79), 467-480. https://doi.org/10.18800/themis.202101.027

Fernández, H. (2014). *Manual de Derecho Informático.* Abeledo Perrot.

Guerrero Argote, C. (2018). *De Budapest al Perú: análisis sobre el proceso de implementación del convenio de ciberdelincuencia.* Hiperderecho. https://www.derechosdigitales.org/wp-content/uploads/minuta_hiperderecho.pdf

Guerrero, G. y Guerrero, C. (2014). *Metodología de la investigación.* Grupo Editorial Patria.

Guerrero Peralta, O. (2007). *Fundamentos Teóricos Constitucionales del Nuevo Sistema Penal.* Ediciones Nueva jurídica.

Hernández, R. (2018). *Metodología de la Investigación. Las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill

Kleiman, H. y Tello, P. (2018). ¿Existe un bien jurídico para los delitos informáticos? Reunión Preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP). *Grupo argentino, Facultad de Derecho, UBA,* (1), 37-45.

Lunarejo, E. y Rodríguez, K. (2021). *El levantamiento del secreto de las comunicaciones en los delitos informáticos* [Tesis de grado]. Repositorio Institucional Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/76869

Marco Urgell, A. (2010). *La intervención de las comunicaciones telefónicas: grabación de las conversaciones propias, hallazgos casuales y consecuencias jurídicas derivadas de la ilicitud de la injerencia* [Tesis de grado]. Repositorio Institucional Universidad Autónoma de Barcelona.

Martínez, M. (2018). *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil.* Erreius.

Mayer, L. y Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología, 9*(1), 151-184. https://doi.org/10.5354/0719-2584.2020.53447

Mazuelos, J. (2001). Los delitos informáticos: una aproximación a la regulación del Código Penal Peruano. *Revista de doctrina y jurisprudencia penales, (2).*

Ministerio de Justicia y Derechos Humanos. (2022). *Ciberdelincuencia Reporte de Información Estadística y Recomendaciones para la Prevención.* Observatorio Nacional de Política Criminal.

Mitran, G. (2021). *La intervención de las comunicaciones telefónicas y telemáticas* [Tesis de grado]. Repositorio Institucional Universidad de Almería. https://repositorio.ual.es/handle/10835/13187

Montero, J. (1999). *La intervención de las comunicaciones telefónicas en el proceso penal.* Tirant lo blanch.

Monzón, W. (2015). Derecho a la intimidad, secreto de las comunicaciones y poder de dirección. *Gaceta penal y procesal penal,* (95), 104-115.

Noya, L. (2000). *La intervención de comunicaciones orales directas en el proceso penal.* Tirant lo Blanch.

Ñaupa, H., Marcelino, V., Palacios, J. y Romero, H. (2018). *Metodología de la investigación Cuantitativa-Cualitativa. Redacción de la Tesis.* Ediciones de la U.

Peña, O. y Almanza, F. (2010). *Teoría del Delito.* Asociación Peruana de Ciencias Jurídicas y Conciliación. https://derecho.usmp.edu.pe/wp-content/uploads/2022/05/libro-teoria-del-delito-oscar-pena.pdf

Peña Cabrera, A. (2011). *Derecho procesal penal, Sistema acusatorio, teoría del caso y técnicas de litigación oral.* Editorial Rodhas.

Pérez, J. (2019). *Delitos regulados en leyes penales.* Gaceta Jurídica.

Prado, V. (2018). *La dosimetría del castigo penal.* Ideas Solución Editorial.

Quiñonez, J. y Marlon, V. (2015). Constitución, privacidad y geolocalización. *Actualidad Constitucional,* (94), 215-221.

Ramos, C. (2018). *Cómo hacer una tesis en derecho y no envejecer en el intento.* Lex&Iuris

Ramos, C. (2020). Los alcances de una investigación. *Ciencia América, 9*(3), 1-5. https://doi.org/10.33210/ca.v9i3.336

Rayón, M. y Gómez, J. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario jurídico y económico escurialense, 47*(34), 209-234.

Recurso de apelación N° 04-2015 "3" (Corte Suprema de Justicia de la Republica Sala Penal Especial).

Ríos, C. (2019). Guía para la realización de trabajos de investigación. Universidad Continental, 72.

Romboli, R. (2017). *Justicia constitucional, derechos fundamentales y tutela judicial.* Palestra.

Rosas, J. (2016). *La prueba en el Nuevo Código Procesal Penal.* Editorial Legales.

Salcedo, C. (2012). Intervención de las comunicaciones telefónicas como método auxiliar de la investigación fiscal. *Investigación en Ciencias Jurídicas y Sociales,* (2), 75-92. https://ojs.ministeriopublico.gov.py/index.php/rjmp/article/view/17/338

San Martín, C. (2015). *Derecho Procesal Penal. Lecciones.* Fondo editorial del INPECCP.

Sifuentes, R. (2022). *Informe sobre la Resolución N°2272-2018/SPC-INDECOPI.* Pontificia Universidad Católica del Perú, 74. http://hdl.handle.net/20.500.12404/23140

Sori, F. (2003). *Fullmetal Alchemist* [Película].

STC Exp. N° 0045-2005-PI/TC (Tribunal Constitucional, 2005).

STC Exp. N° 00655-2010-PHC/TC (Tribunal Constitucional, 2010).

Strauss, A. y Corbin, J. (2001). *Bases de la investigación cualitativa. Técnicas y procedimientos para desarrollar la teoría fundamentada.* Universidad de Antioquía.

UETI-CPP. (s.f.). *UETI-CPP/Información Institucional.* Unidad de equipo técnico institucional del Código Procesal Penal. https://www.pj.gob.pe/wps/wcm/connect/NCPP/s_ncpp/as_info/

Varona, A. (2020). Aspectos relevantes de la interceptación de las comunicaciones telefónicas. *IusInkarri, 9*(9), 237-258.

Villavicencio, F. (2014). Delitos informáticos. *Ius et veritas,* (49), 284-304. https://doi.org/https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Villegas, E. (2016). El derecho al secreto de las comunicaciones y la prueba ilícita en el proceso penal: a propósito del R.N. N° 2076-2014 -Lima Norte. *Gaceta Penal y Procesal Penal,* (85), 313-331.

Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius et praxis,* (53), 95-110. https://doi.org/10.26439/iusetpraxis2021.n053.4995

ANEXOS

ANEXO 1. Matriz de Consistencia

<table>
<tr><td colspan="2">Título preliminar: El tratamiento de los concursos de delitos, sobre los delitos cometidos como medio para cometer otros en nuestra legislación penal nacional</td></tr>
<tr><td>Problemas</td><td>Objetivos de la investigación</td></tr>
<tr><td>General
¿De qué manera afecta la exigencia del requisito de suma pena previsto en el numeral 1 del artículo 230 del Código Procesal Penal para la autorización judicial de levantamiento de secreto de las comunicaciones en su forma de información histórica, en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo, periodo 2021 y 2022?</td><td>General
Examinar como la exigencia del requisito de suma pena previsto en el numeral 1 del artículo 230 del Código Procesal Penal para la autorización judicial de levantamiento de secreto de las comunicaciones en su forma de información histórica, afecta en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo, periodo 2021 y 2022.</td></tr>
<tr><td>Específicos
• ¿En qué medida el requisito de suma pena restringe la procedibilidad de los requerimientos fiscales de levantamiento de secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo, periodo 2021 y 2022?
• ¿Cuál es el grado de lesividad de la medida restrictiva de derechos de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo, periodo 2021 y 2022?</td><td>Específicos
• Determinar en qué medida el requisito de suma pena restringe la procedibilidad de los requerimientos fiscales de levantamiento de secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo, periodo 2021 y 2022.
• Determinar el grado de lesividad de la medida restrictiva de derechos de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático en los juzgados comunes de investigación preparatoria de Huancayo, periodo 2021 y 2022.</td></tr>
</table>

<table>
<tr><th colspan="4">Diseño metodológico</th></tr>
<tr><th>Metodología</th><th>Enfoque</th><th>Diseño de la investigación</th><th>Técnicas e instrumentos de recojo de información</th></tr>
<tr><td>1. Método dogmático
2. Método sociológico funcional</td><td>Enfoque cualitativo</td><td>1. Propósito intrínseco: descriptiva y explicativa.
2. Propósito extrínseco: teórica o pura</td><td>La técnica utilizada para el recojo de información fue la entrevista.
Como instrumento de recolección de datos se utilizó la guía de entrevista.</td></tr>
<tr><th colspan="4">Población y muestra</th></tr>
<tr><td colspan="2">Criterios de inclusión: Tres jueces de investigación preparatoria y tres fiscales del distrito judicial y fiscal de Junín, que conocen casos sobre el delito de fraude informático y levantamientos del secreto de las comunicaciones.</td><td colspan="2">Criterios de exclusión: No se tomó en cuenta a especialistas, asistentes jurisdiccionales ni asistentes en función fiscal que conocen el ámbito de levantamientos del secreto de las comunicaciones.</td></tr>
<tr><th colspan="2">Objetivos</th><th colspan="2">Categorías</th></tr>
<tr><td colspan="2">Los objetivos del análisis documental son los siguientes:
1. Obtener información fiable sobre el delito de fraude informático y su especial necesidad para levantar el secreto de las comunicaciones, teniendo en cuenta sus tipos, necesidad y lesividad; todo ello con la información de libros, tesis, artículos científicos, conferencias magistrales, y expedientes judiciales de la CSJJU Después de sistematizar y analizar la información recabada, utilizar la información para plantear una solución al problema.</td><td colspan="2">1. Levantamiento del secreto de las comunicaciones.
2. Delito de fraude informático.</td></tr>
<tr><th colspan="2">Bibliografía de sustento para la justificación y delimitación del problema</th><th colspan="2">Bibliografía de sustento usada para el diseño metodológico</th></tr>
<tr><td colspan="2">Blancas, G. (2012). Medidas a seguir para el levantamiento del secreto de las comunicaciones y telecomunicaciones (arts 230 y 231 del NCCP). Horizonte Empresarial, (10), 63-72. https://doi.org/10.31381/horizonte_empresarial.v0i10.248</td><td colspan="2">Croda, J. y Abad, E. (2016). Modelos de investigación cualitativa y cuantitativa y su aplicación en el estudio del derecho. Revista electrónica de investigación de la Universidad de Xalapa, (4), 12.</td></tr>
</table>

Castillo, J. L. (2022). Notas sobre el contenido esencial del articulo 2.10 de la Constitucion sobre el derecho a la inviolavilidad de las comunicaciones en el proceso penal. *Gaceta penal y procesal penal*(158), 265-272.

Diaz, F. (2006). El derecho fundamental al secreto de las comunicaciones. *Derecho PUCP (Revista de la facultad de derecho)*, 159-175. https://doi.org/10.18800/derechopucp.200601.007

Villavicencio, F. (2014). Delitos informáticos. *Ius et veritas* (49), 284-204 https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Ñaupa, H., Marcelino, V., Palacios, J. y Romero, H. (2018). *Metodología de la investigación Cuantitativa-Cualitativa-Redaccion de la Tesis* (5 ed.). Ediciones de la U.

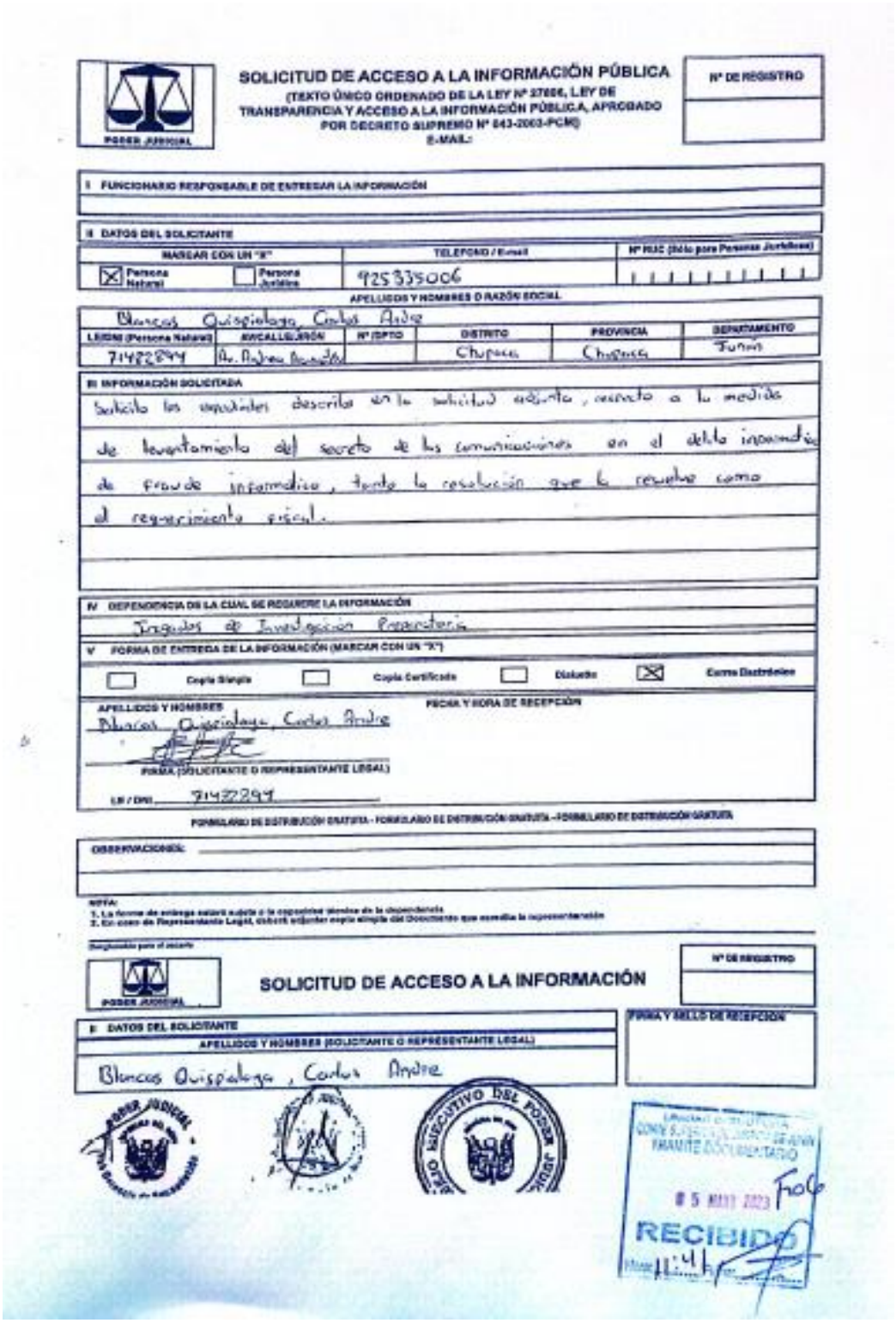
Ramos, C. (2018). *Como hacer una tesis en derecho y no envejecer en el intento.* Grupo Editorial Lex & Iuris S.A.C.

Ramos, C. (2020). Los alcances de una investigacion. *CienciaAmerica, 9*(3), 1-5. https://doi.org/10.33210/ca.v9i3.336

Rios, C. (2019). Guía para la realización de trabajos de investigación. *Universidad Continental*, 72.

Strauss, A. y Corbin J. (2001). *Bases de la investigacion cualitativa.Tecnicas y procedimientos para desarrollar la teoria fundamentada.* Universidad de Antioquia.

ANEXO 2. Solicitud de acceso a la información



PODER JUDICIAL

SOLICITUD DE ACCESO A LA INFORMACIÓN PÚBLICA

(TEXTO ÚNICO ORDENADO DE LA LEY Nº 27806, LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, APROBADO POR DECRETO SUPREMO Nº 043-2003-PCM)

E-MAIL:

Nº DE REGISTRO

I FUNCIONARIO RESPONSABLE DE ENTREGAR LA INFORMACIÓN

II DATOS DEL SOLICITANTE

MARCAR CON UN "X"		TELEFONO / E-mail	Nº RUC (Solo para Personas Jurídicas)
[X] Persona Natural	[ ] Persona Jurídica	925335006	

APELLIDOS Y NOMBRES O RAZÓN SOCIAL

Blancas Quispelaya, Carlos Andre

LE/DNI (Persona Natural)	AVICALLE/JIRÓN	Nº /DPTO	DISTRITO	PROVINCIA	DEPARTAMENTO
71482894	Av. Ruben Acevedo		Chupaca	Chupaca	Junin

III INFORMACIÓN SOLICITADA

Solicito los requisitos descritos en la solicitud adjunta, respecto a la medida de levantamiento del secreto de las comunicaciones en el delito informático de fraude informatico, tanto la resolución que la resuelve como el requerimiento fiscal.

IV DEPENDENCIA DE LA CUAL SE REQUIERE LA INFORMACIÓN

Juzgados de Investigación Preparatoria

V FORMA DE ENTREGA DE LA INFORMACIÓN (MARCAR CON UN "X")

[ ] Copia Simple [ ] Copia Certificada [ ] Diskette [X] Correo Electrónico

APELLIDOS Y NOMBRES

Blancas Quispelaya, Carlos Andre

FIRMA (SOLICITANTE O REPRESENTANTE LEGAL)

LE / DNI 71482894

FECHA Y HORA DE RECEPCIÓN

FORMULARIO DE DISTRIBUCIÓN GRATUITA - FORMULARIO DE DISTRIBUCIÓN GRATUITA - FORMULARIO DE DISTRIBUCIÓN GRATUITA

OBSERVACIONES:

NOTA:
1. La forma de entrega estará sujeta a la capacidad técnica de la dependencia
2. En caso de Representante Legal, deberá adjuntar copia simple del Documento que acredita la representación

Designación para el estado

PODER JUDICIAL

SOLICITUD DE ACCESO A LA INFORMACIÓN

Nº DE REGISTRO

II DATOS DEL SOLICITANTE

APELLIDOS Y NOMBRES (SOLICITANTE O REPRESENTANTE LEGAL)

Blancas Quispelaya, Carlos Andre

FIRMA Y SELLO DE RECEPCIÓN

PODER JUDICIAL

PODER EJECUTIVO DEL PODER JUDICIAL

05 MAY 2023

RECIBIDO

Hora 11:41

Solicito: Acceso a información pública para la revisión de los expedientes judiciales sobre levantamiento del secreto de las comunicaciones en el delito de fraude informático.

AL ÓRGANO COMPETENTE DE LA CORTE SUPERIOR DE JUSTICIA DE JUNÍN

Carlos Andre Blancas Quispialaya, identificado con DNI 71482894, bachiller en derecho por la Universidad Continental, con domicilio en la avenida Andres Arauco S/N, distrito y provincia de Chupaca, con número de celular 925335006 y con correo electrónico personal andreblancasquispialaya@gmail.com me dirijo a usted. respetuosamente a fin de señalar lo siguiente:

Que, en amparo a la Ley de Transparencia y acceso a la Información Pública prevista en la Ley N° 27806 y su reglamento, recurro ante vuestra digna institución con el fin de solicitar la autorización correspondiente a fin de revisar y analizar los expedientes sobre el delito de fraude informático y el incidente sobre levantamiento del secreto de las comunicaciones de los juzgados de investigación preparatoria en los años 2021 y 2022 a efectos de obtener datos que sustenten la investigación titulada *"Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático"*, para optar el titulo profesional de abogado, por lo que para lograr tal cometido se requiere tener el permiso para revisar los siguientes expedientes:

N°	Expediente	Incidente
1	00097-2021-64-1501-JR-PE-01	Levantamiento del secreto de las comunicaciones.
2	01042-2022-91-1501-JR-PE-01	Levantamiento del secreto de las comunicaciones.
3	01198-2021-79-1501-JR-PE-02	Levantamiento del secreto de las comunicaciones.
4	01314-2021-40-1501-JR-PE-07	Levantamiento del secreto de las comunicaciones.
5	01467-2021-10-1501-JR-PE-07	Levantamiento del secreto de las comunicaciones.
6	01873-2022-41-1501-JR-PE-06	Levantamiento del secreto de las comunicaciones.
7	02297-2021-59-1501-JR-PE-06	Levantamiento del secreto de las comunicaciones.
8	02449-2021-6-1501-JR-PE-02	Levantamiento del secreto de las comunicaciones.
9	02562-2022-63-1501-JR-PE-02	Levantamiento del secreto de las comunicaciones.
10	02704-2021-94-1501-JR-PE-06	Levantamiento del secreto de las comunicaciones.
11	03072-2022-11-1501-JR-PE-02	Levantamiento del secreto de las comunicaciones.
12	03866-2021-44-1501-JR-PE-01	Levantamiento del secreto de las comunicaciones.

13	04194-2022-59-1501-JR-PE-01	Levantamiento del secreto de las comunicaciones.

POR LO EXPUESTO:

Solicito el acceso a la información publica sobre los expedientes en materia penal, en los que se siguen por el delito de fraude informático, precisando que lo solicitado tiene únicamente fines académicos, en este sentido los datos obtenidos se mantendrán en total confidencialidad. Sin otro particular me despido solicitando tenga a bien dar por fundada mi petición lo cual implica la finalidad que mi persona desea alcanzar

ANEXOS:

1. Resolución Decanal Nº 425-2023-FD-UC, aprobación del plan de tesis de la solicitante emitida por la Universidad Continental
2. Grado de Bachiller emitida por la Universidad Continental en la facultad de Derecho
3. Copia simple de DNI del solicitante

71482894

ANEXO 3. Oficio N° 000114-2023-MNCPP-GAD-CSJJU-PJ.

Presidencia de la Corte Superior de Justicia de Junin
Gerencia de Administracion Distrital

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la unidad, la paz y el desarrollo"

Firma Digital

El Tambo, 29 de Mayo del 2023

OFICIO N° 000114-2023-MNCPP-GAD-CSJJU-PJ

Sr(a).
EDISON FRANK ORUDNAP ARANA
Responsable del Portal de Transparencia Estándar y Acceso a la Información Pública

Presente. -

Asunto :Sobre solicitud de acceso a la información pública para la revisión de los expedientes judiciales sobre levantamiento del secreto de las comunicaciones en el delito de fraude informático..

Referencia :EXPEDIENTE002142-2023-MUP-GA
HOJA DE ENVIO 000489-2023-MNCPP-GAD-CSJJU (18MAY2023)

Tengo el agrado de dirigirme a usted, para saludarlo muy cordialmente y manifestarle que, en atención al asunto y en relación al documento de la referencia, mediante el cual señala que se ha recepcionado una solicitud de acceso a la información pública presentada al amparo de la Ley Nro. 27806 – Ley de Transparencia y Acceso a la Información Publica presentada por la persona de Carlos Andre Blancas Quispialaya quien solicita autorización a fin de revisar y analizar los expedientes que a continuación se señalaran que se encuentran en trámite en su Juzgado a efectos de obtener datos para sustentar la investigación titulada "Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático".

De la revisión del listado presentado por la persona de Carlos Andre Blancas Quispialaya en su solicitud se pueden advertir trece (13) expedientes, cuyos incidentes se tratan del levantamiento de secreto de comunicaciones, los cuales de la revisión en el sistema no se encuentran en etapa de ejecución, lo que significa que siguen en trámite su investigación.

Al respecto es preciso señalar que, la reserva de la investigación se tiene entendida como una limitación que impide que cualquier persona extraña al proceso pueda tomar conocimiento de él mientras se desarrolla la investigación, de acuerdo a lo establecido por el artículo 324.1 del Código Procesal Penal esta limitación se extiende inclusive a los sujetos procesales que aún no se han hecho parte del proceso.

El artículo precitado establece expresamente que "[…] Sólo podrán enterarse de su contenido las partes de manera directa o a través de sus abogados debidamente acreditados en autos. […]". De lo que se desprende que un sujeto procesal no acreditado (es decir que aún no es parte) no podrá acceder a la carpeta fiscal o al expediente judicial de ser el caso.

Presidencia de la Corte Superior de Justicia de Junin
Gerencia de Administracion Distrital

Aunado a ello se trata de incidentes de levantamiento del secreto de comunicaciones procesos que tienen el carácter de reservado de conformidad al inciso 3 del artículo 230° del Código procesal Penal, por lo que no resulta atendible lo requerido por Carlos Andre Blancas Quispialaya.

Sin otro particular, hago propicia la oportunidad, para reiterar a usted los sentimientos de mi mayor consideración.

Atentamente,

Documento firmado digitalmente

MIRIAM ROSARIO ZARATE PAUCARPURA
Administrador del Modulo del Nuevo Codigo Procesal Penal
Presidencia de la Corte Superior de Justicia de Junin

ANEXO 4. Formato de ficha de validación de instrumento.

VALIDACION DE INSTRUMENTO
CARTA DE PRESENTACION

Huancayo, 20 de julio de 2023

Señor:

Asunto: Validación de instrumento a través de juicio de experto.

Presente.-

Me es muy grato dirigirme a usted para expresarle un cordial saludo, me dirijo a usted para comentarle que, en mi calidad de bachiller en Derecho por la Universidad Continental, requiero validar el instrumento con el cual recogeré la información necesaria para poder ejecutar el desarrollo de mi tesis para optar por el título profesional de abogado.

El titulo de mi tesis es: "Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático", siendo indispensable contar con la aprobación de docentes especializados para poder validar el instrumento y poder ejecutar la investigación en mención, y habiendo considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación.

Se adjunta al expediente de validación, los siguientes:

1. Carta de presentación.
2. Matriz de consistencia del estudio.
3. Ficha de validación
4. Cuestionario
5. Ficha de análisis

Agradezco sinceramente su tiempo y consideración al revisar mi solicitud. Espero con entusiasmo su valiosa evaluación la cual me acercará a la culminación de mi tesis para obtener el título profesional de abogado, me despido de usted expresándole mi más alto grado de respeto y consideración.

Atentamente

Blancas Quispialaya, Carlos Andre
DNI N° 71482894

FICHA DE VALIDACIÓN DE INSTRUMENTO POR EXPERTO

I. DATOS GENERALES

1.1. **Título de la investigación:** Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.

1.2. **Nombre del instrumento:** Encuestas.

1.3. **Nombres y apellidos del investigador:** Carlos Andre Blancas Quispialaya.

II. CRITERIOS PARA VALIDACIÓN DE LOS INSTRUMENTOS (Marcar con una X)

ASPECTOS DE VALIDACIÓN														
CRITERIOS	**INDICADORES**	**INACEPTABLE**						**MINIMAMENTE ACEPTABLE**			**ACEPTABLE**			
		40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Se evidencia una formulación de los ítems con un lenguaje claro y comprensible													
OBJETIVIDAD	Los ítems incluidos son objetivos y evitan juicios o interpretaciones subjetivas del investigador.													
ACTUALIDAD	Los ítems incluidos evalúan una temática actual y relevante en el campo de estudio.													
ORGANIZACIÓN	Los ítems se encuentran organizados de una manera lógica y adecuada.													
SUFICIENCIA	Los ítems tienen la capacidad para recopilar la información requerida y proporcionar datos confiables y válidos.													
INTENCIONALIDAD	Se evidencia en los ítems la claridad y coherencia en las intenciones y objetivos investigativos que persiguen.													
CONSISTENCIA	Los ítems que conforman el instrumento están correlacionados entre sí y buscan la obtención de resultados consistentes.													

COHERENCIA	Los ítems capturan de manera precisa y completa la información necesaria para abordar coherentemente las preguntas de investigación y los objetivos planteados.													
METODOLOGÍA	La elaboración de los ítems se realizó con el uso de métodos y procedimientos apropiados que buscan obtener datos válidos y significativos.													
PERTINENCIA	El instrumento es apropiado y adecuado para obtener información necesaria en el contexto de una investigación cualitativa													

III. OPINIÓN DE APLICABILIDAD (Marcar con una X)

El instrumento **cumple** con los requisitos para su aplicación	
El instrumento **no cumple** con los requisitos para su aplicación	

IV. PROMEDIO DE VALORACIÓN

Nombre del instrumento	**Encuestas**
Objetivo del instrumento	Analizar los criterios adoptados por los jueces y fiscales de Huancayo, respecto al levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático
Nombres y apellidos del experto	
Título profesional	
Dirección domiciliaria	
Grado académico	

Firma		**Lugar y fecha**	

Cuestionario

Nombres y Apellidos: _____

Título de la tesis: Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.

1. ¿Qué concepción tiene sobre el levantamiento del secreto de las comunicaciones?

2. ¿Qué concepción tiene sobre los delitos informáticos y el delito de fraude informático en particular?

3. ¿Considera que el levantamiento del secreto de las comunicaciones es indispensable para las investigaciones en delitos informáticos?

4. En su experiencia: ¿Cómo afecta la exigencia del requisito de una sanción penal superior a cuatro años de pena privativa de libertad establecida en el numeral 1 del artículo 230 del Código Procesal Penal, para la autorización judicial de levantamiento de secreto de las

comunicaciones en su forma de información histórica en los casos relacionados con el delito de fraude informático que conoció su despacho?

5. ¿Cuáles son los criterios que se utiliza para aplicar el requisito de suma pena en la autorización judicial de levantamiento de secreto de las comunicaciones, con respecto a la pena establecida en el delito de fraude informático?

6. En su experiencia: ¿Ha observado algún impacto negativo en la investigación de delitos de fraude informático debido al posible rechazo de los requerimientos fiscales por no cumplir con el requisito de suma pena para el levantamiento del secreto de las comunicaciones?

7. ¿Considera que el límite impuesto como presupuesto material de suma pena o prognosis de pena para el levantamiento del secreto de las comunicaciones en su forma de información histórica podría afectar la identificación y persecución de los responsables del delito de fraude informático?

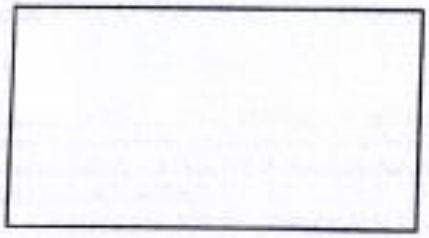
8. Respecto a la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional: ¿Considera que para la autorización judicial del levantamiento de secreto de las comunicaciones en los delitos informáticos aún se debe tener en cuenta los requisitos establecidos en dicha ley, o sólo el previsto en numeral 1 del artículo 230 del Código Penal, o ambas?

9. ¿Cuál es su perspectiva sobre equilibrar (ponderar) la lesión de los derechos fundamentales del secreto e inviolabilidad de las comunicaciones con la necesidad de investigar y esclarecer adecuadamente el delito de fraude informático?

10. ¿Cuál es la evaluación general sobre el grado de lesividad de la medida restrictiva de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático, considerando los intereses del Estado y los derechos fundamentales de las personas involucradas?

11. ¿Considera usted que existen grados de lesión en la restricción a los derechos fundamentales de los afectados en la intervención de las comunicaciones como la interceptación de las comunicaciones en tiempo real, geolocalización e información histórica?

12. En su experiencia, ¿Existe alguna diferencia en los criterios que se utilizan para resolver requerimientos de levantamiento del secreto de las comunicaciones en su forma de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica, o se utiliza el mismo criterio?



Firma y Sello

ANEXO 5. Ficha de validación de instrumento por primer experto: Mg. Héctor Ramiro Marinovich Ventocilla.

VALIDACION DE INSTRUMENTO
CARTA DE PRESENTACION

Huancayo, 20 de julio de 2023

Señor: Hector Ramiro Marinovich Ventocilla

Asunto: Validación de instrumento a través de juicio de experto.

Presente.-

Me es muy grato dirigirme a usted para expresarle un cordial saludo, me dirijo a usted para comentarle que, en mi calidad de bachiller en Derecho por la Universidad Continental, requiero validar el instrumento con el cual recogeré la información necesaria para poder ejecutar el desarrollo de mi tesis para optar por el título profesional de abogado.

El título de mi tesis es: "Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático", siendo indispensable contar con la aprobación de docentes especializados para poder validar el instrumento y poder ejecutar la investigación en mención, y habiendo considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación.

Se adjunta al expediente de validación, los siguientes:

1. Carta de presentación.
2. Matriz de consistencia del estudio.
3. Ficha de validación
4. Cuestionario
5. Ficha de análisis

Agradezco sinceramente su tiempo y consideración al revisar mi solicitud. Espero con entusiasmo su valiosa evaluación la cual me acercará a la culminación de mi tesis para obtener el título profesional de abogado, me despido de usted expresándole mi más alto grado de respeto y consideración.

Atentamente

Blancas Quispialaya, Carlos Andre
DNI N° 71482894

FICHA DE VALIDACIÓN DE INSTRUMENTO POR EXPERTO

I. DATOS GENERALES

1.1. **Título de la investigación:** Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.

1.2. **Nombre del instrumento:** Encuestas.

1.3. **Nombres y apellidos del investigador:** Carlos Andre Blancas Quispialaya.

II. CRITERIOS PARA VALIDACIÓN DE LOS INSTRUMENTOS (Marcar con una X)

ASPECTOS DE VALIDACIÓN														
CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Se evidencia una formulación de los ítems con un lenguaje claro y comprensible												X	
OBJETIVIDAD	Los ítems incluidos son objetivos y evitan juicios o interpretaciones subjetivas del investigador												X	
ACTUALIDAD	Los ítems incluidos evalúan una temática actual y relevante en el campo de estudio												X	
ORGANIZACIÓN	Los ítems se encuentran organizados de una manera lógica y adecuada												X	
SUFICIENCIA	Los ítems tienen la capacidad para recopilar la información requerida y proporcionar datos confiables y válidos.												X	
INTENCIONALIDAD	Se evidencia en los ítems la claridad y coherencia en las intenciones y objetivos investigativos que persiguen.												X	
CONSISTENCIA	Los ítems que conforman el instrumento están correlacionados entre sí y buscan la obtención de resultados consistentes.												X	

COHERENCIA	Los ítems capturan de manera precisa y completa la información necesaria para abordar coherentemente las preguntas de investigación y los objetivos planteados.												X	
METODOLOGÍA	La elaboración de los ítems se realizó con el uso de métodos y procedimientos apropiados que buscan obtener datos válidos y significativos.												X	
PERTINENCIA	El instrumento es apropiado y adecuado para obtener información necesaria en el contexto de una investigación cualitativa.												X	

III. OPINIÓN DE APLICABILIDAD (Marcar con una X)

El instrumento **cumple** con los requisitos para su aplicación	X
El instrumento **no cumple** con los requisitos para su aplicación	

IV. PROMEDIO DE VALORACIÓN 95

Nombre del instrumento	**Encuestas**		
Objetivo del instrumento	Analizar los criterios adoptados por los jueces y fiscales de Huancayo, respecto al levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático		
Nombres y apellidos del experto	HECTOR ROMERO MARINOVICH VENTOCILLA .		
Título profesional	ABOGADO .		
Dirección domiciliaria	JR. CIRCUITO LOS HEROES 871. EL TAMBO .		
Grado académico	MAGISTER.		
Firma	HECTOR ROMERO MARINOVICH VENTOCILLA ABOGADO CAJ. 3017	**Lugar y fecha**	HUANCAYO 01/08/2023

ANEXO 6. Ficha de validación de instrumento por segundo experto: Mg. Pedro Raúl Cunyas Enríquez.

VALIDACION DE INSTRUMENTO
CARTA DE PRESENTACION

Huancayo, 20 de julio de 2023

Señor: Pedro Raul Cunyas Enriquez

Asunto: Validación de instrumento a través de juicio de experto.

Presente.-

Me es muy grato dirigirme a usted para expresarle un cordial saludo, me dirijo a usted para comentarle que, en mi calidad de bachiller en Derecho por la Universidad Continental, requiero validar el instrumento con el cual recogeré la información necesaria para poder ejecutar el desarrollo de mi tesis para optar por el título profesional de abogado.

El titulo de mi tesis es: "Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático", siendo indispensable contar con la aprobación de docentes especializados para poder validar el instrumento y poder ejecutar la investigación en mención, y habiendo considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación.

Se adjunta al expediente de validación, los siguientes:

1. Carta de presentación.
2. Matriz de consistencia del estudio.
3. Ficha de validación
4. Cuestionario
5. Ficha de análisis

Agradezco sinceramente su tiempo y consideración al revisar mi solicitud. Espero con entusiasmo su valiosa evaluación la cual me acercará a la culminación de mi tesis para obtener el título profesional de abogado, me despido de usted expresándole mi más alto grado de respeto y consideración.

Atentamente

Blancas Quispialaya, Carlos Andre
DNI N° 71482894

FICHA DE VALIDACIÓN DE INSTRUMENTO POR EXPERTO

I. DATOS GENERALES

1.1. **Título de la investigación:** Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.
1.2. **Nombre del instrumento:** Encuestas.
1.3. **Nombres y apellidos del investigador:** Carlos Andre Blancas Quispialaya.

II. CRITERIOS PARA VALIDACIÓN DE LOS INSTRUMENTOS (Marcar con una X)

ASPECTOS DE VALIDACIÓN														
CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Se evidencia una formulación de los ítems con un lenguaje claro y comprensible												X	
OBJETIVIDAD	Los ítems incluidos son objetivos y evitan juicios o interpretaciones subjetivas del investigador.												X	
ACTUALIDAD	Los ítems incluidos evalúan una temática actual y relevante en el campo de estudio.												X	
ORGANIZACIÓN	Los ítems se encuentran organizados de una manera lógica y adecuada.												X	
SUFICIENCIA	Los ítems tienen la capacidad para recopilar la información requerida y proporcionar datos confiables y válidos.												X	
INTENCIONALIDAD	Se evidencia en los ítems la claridad y coherencia en las intenciones y objetivos investigativos que persiguen.												X	
CONSISTENCIA	Los ítems que conforman el instrumento están correlacionados entre sí y buscan la obtención de resultados consistentes.												X	

COHERENCIA	Los ítems capturan de manera precisa y completa la información necesaria para abordar coherentemente las preguntas de investigación y los objetivos planteados.												X		
METODOLOGÍA	La elaboración de los ítems se realizó con el uso de métodos y procedimientos apropiados que buscan obtener datos válidos y significativos.												X		
PERTINENCIA	El instrumento es apropiado y adecuado para obtener información necesaria en el contexto de una investigación cualitativa.												X		

III. OPINIÓN DE APLICABILIDAD (Marcar con una X)

El instrumento **cumple** con los requisitos para su aplicación	X
El instrumento **no cumple** con los requisitos para su aplicación	

IV. PROMEDIO DE VALORACIÓN 95

Nombre del instrumento	**Encuestas**		
Objetivo del instrumento	Analizar los criterios adoptados por los jueces y fiscales de Huancayo, respecto al levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático		
Nombres y apellidos del experto	Pedro Saúl Cuayla Enríquez		
Título profesional			
Dirección domiciliaria	Av. Agustín Morales N° 516-Tambo		
Grado académico	Mg. en Ciencias Penales		
Firma	Mg. Pedro S. Cuayla Enríquez ABOGADO CAL 1592	**Lugar y fecha**	

ANEXO 7. Fichas de validación de instrumento por tercer experto: Abg. David Gutarra Vizzi.

VALIDACION DE INSTRUMENTO
CARTA DE PRESENTACION

Huancayo, 20 de julio de 2023

Señor: David Gutarra Vizzi

Asunto: Validación de instrumento a través de juicio de experto.

Presente.-

Me es muy grato dirigirme a usted para expresarle un cordial saludo, me dirijo a usted para comentarle que, en mi calidad de Bachiller en Derecho por la Universidad Continental, requiero validar el instrumento con el cual recogeré la información necesaria para poder ejecutar el desarrollo de mi tesis para optar por el título profesional de abogado.

El título de mi tesis es: "Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático", siendo indispensable contar con la aprobación de docentes especializados para poder validar el instrumento y poder ejecutar la investigación en mención, y habiendo considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación.

Se adjunta al expediente de validación, los siguientes:

1. Carta de presentación.
2. Matriz de consistencia del estudio.
3. Ficha de validación
4. Cuestionario
5. Ficha de análisis

Agradezco sinceramente su tiempo y consideración al revisar mi solicitud. Espero con entusiasmo su valiosa evaluación la cual me acercará a la culminación de mi tesis para obtener el título profesional de abogado, me despido de usted expresándole mi más alto grado de respeto y consideración.

Atentamente

Blancas Quisplalaya, Carlos Andre
DNI 71482894

FICHA DE VALIDACIÓN DE INSTRUMENTO POR EXPERTO

I. DATOS GENERALES

1.1. **Título de la investigación:** Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.

1.2. **Nombre del instrumento:** Encuestas.

1.3. **Nombres y apellidos del investigador:** Carlos Andre Blancas Quispialaya.

II. CRITERIOS PARA VALIDACIÓN DE LOS INSTRUMENTOS (Marcar con una X)

ASPECTOS DE VALIDACIÓN														
CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Se evidencia una formulación de los ítems con un lenguaje claro y comprensible												X	
OBJETIVIDAD	Los ítems incluidos son objetivos y evitan juicios o interpretaciones subjetivas del investigador.													X
ACTUALIDAD	Los ítems incluidos evalúan una temática actual y relevante en el campo de estudio.												X	
ORGANIZACIÓN	Los ítems se encuentran organizados de una manera lógica y adecuada.												X	
SUFICIENCIA	Los ítems tienen la capacidad para recopilar la información requerida y proporcionar datos confiables y válidos.												X	
INTENCIONALIDAD	Se evidencia en los ítems la claridad y coherencia en las intenciones y objetivos investigativos que persiguen.												X	
CONSISTENCIA	Los ítems que conforman el instrumento están correlacionados entre sí y buscan la obtención de resultados consistentes.												X	

COHERENCIA	Los ítems capturan de manera precisa y completa la información necesaria para abordar coherentemente las preguntas de investigación y los objetivos planteados.												X	
METODOLOGÍA	La elaboración de los ítems se realizó con el uso de métodos y procedimientos apropiados que buscan obtener datos válidos y significativos.												X	
PERTINENCIA	El instrumento es apropiado y adecuado para obtener información necesaria en el contexto de una investigación cualitativa.												X	

III. OPINIÓN DE APLICABILIDAD (Marcar con una X)

El instrumento **cumple** con los requisitos para su aplicación	X
El instrumento **no cumple** con los requisitos para su aplicación	

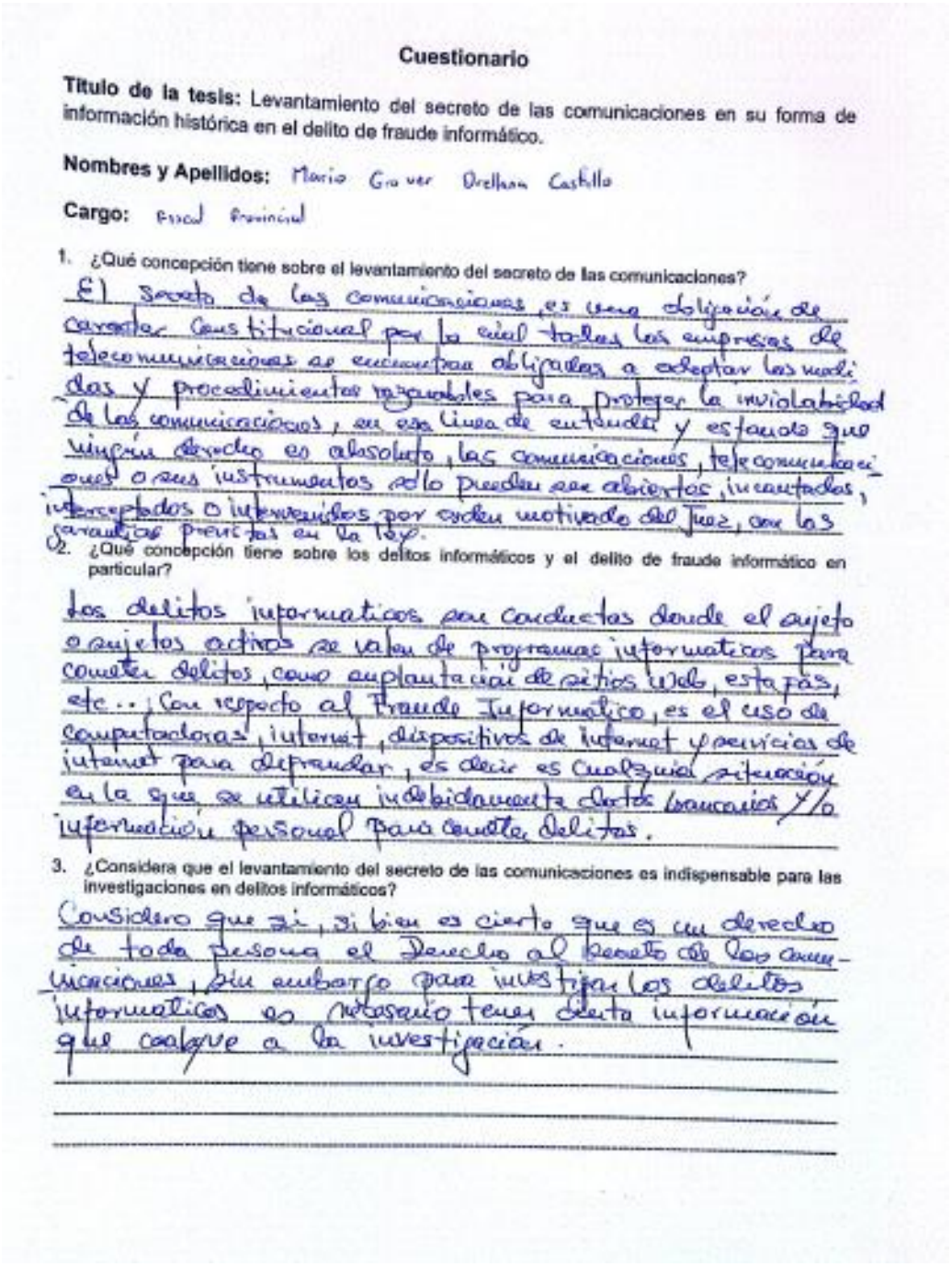
IV. PROMEDIO DE VALORACIÓN 95

Nombre del instrumento	**Encuestas**
Objetivo del instrumento	Analizar los criterios adoptados por los jueces y fiscales de Huancayo, respecto al levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático
Nombres y apellidos del experto	David Gutarra Vizzi
Título profesional	Abogado
Dirección domiciliaria	Calle Eco J # 467 07 200 - El Tambo
Grado académico	Título Abogado

Firma		**Lugar y fecha**	

David Gutarra Vizzi
ABOGADO
CAJ. 4118

ANEXO 8. Cuestionario desarrollado por el fiscal provincial Mario Grover Orellana Castillo



Cuestionario

Título de la tesis: Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.

Nombres y Apellidos: Mario Grover Orellana Castillo

Cargo: Fiscal Provincial

1. ¿Qué concepción tiene sobre el levantamiento del secreto de las comunicaciones?

El Secreto de las comunicaciones, es una obligación de carácter Constitucional por la cual todas las empresas de telecomunicaciones se encuentran obligadas a adoptar las medidas y procedimientos razonables para proteger la inviolabilidad de las comunicaciones, en esa línea de entender y estando que ningún derecho es absoluto, las comunicaciones, telecomunicaciones o sus instrumentos solo pueden ser abiertas, incautadas, interceptadas o intervenidas por orden motivada del Juez, con las garantías previstas en la ley.

2. ¿Qué concepción tiene sobre los delitos informáticos y el delito de fraude informático en particular?

los delitos informaticos son conductas donde el sujeto o sujetos activos se valen de programas informaticos para cometer delitos, como suplantación de sitios Web, estafas, etc.. ; Con respecto al Fraude Informatico, es el uso de computadoras, internet, dispositivos de internet y servicios de internet para defraudar, es decir es cualquier situación en la que se utilicen indebidamente datos bancarios y/o información personal para cometer delitos.

3. ¿Considera que el levantamiento del secreto de las comunicaciones es indispensable para las investigaciones en delitos informáticos?

Considero que si, si bien es cierto que es un derecho de toda persona el Derecho al secreto de las comunicaciones, sin embargo para investigar los delitos informaticos es necesario tener dicha información que coadyuve a la investigación.

4. En su experiencia: ¿Cómo afecta la exigencia del requisito de una sanción penal superior a cuatro años de pena privativa de libertad establecida en el numeral 1 del artículo 230 del Código Procesal Penal, para la autorización judicial de levantamiento de secreto de las comunicaciones en su forma de información histórica en los casos relacionados con el delito de fraude informático que conoció su despacho?

Lo señalado en el artículo 230, se refiere a la intervención y grabación de las comunicaciones y no al levantamiento del secreto de las comunicaciones

5. ¿Cuáles son los criterios que se utiliza para aplicar el requisito de suma pena en la autorización judicial de levantamiento de secreto de las comunicaciones, con respecto a la pena establecida en el delito de fraude informático?

Al determinarse la pena privativa de libertad mediante lo señalado en la Ley Nº 30076 y 30077 modifica el art. 45 para la determinación de la pena, en tercios, siendo el primer tercio entre 02 años y 04 años y 08 meses y si nos encontramos dentro del tercio intermedio pena ría lo señalado en el numeral 1 del artículo 230 del Código Procesal Penal.

6. En su experiencia: ¿Ha observado algún impacto negativo en la investigación de delitos de fraude informático debido al posible rechazo de los requerimientos fiscales por no cumplir con el requisito de suma pena para el levantamiento del secreto de las comunicaciones?

Hasta el momento no se ha encontrado inconveniente alguno, en razón de que normalmente estos delitos se cometen en banda y/o organización criminal o en concurso con otros delitos, por lo que las penas privativas de libertad de superan.

7. ¿Considera que el límite impuesto como presupuesto material de suma pena o prognosis de pena para el levantamiento del secreto de las comunicaciones en su forma de información histórica podría afectar la identificación y persecución de los responsables del delito de fraude informático?

Considero que no, como se ha señalado anteriormente para el levantamiento del secreto de las comunica-

ciones no es necesario que la pena privativa de libertad sea superior a los cuatro años.

8. Respecto a la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional: ¿Considera que para la autorización judicial del levantamiento de secreto de las comunicaciones en los delitos informáticos aún se debe tener en cuenta los requisitos establecidos en dicha ley, o sólo el previsto en numeral 1 del artículo 230 del Código Penal, o ambas?

Consideramos que si ya que al afectar un Derecho Constitucional, se debe de hacer con todos los requisito, debiendo existir una debida motivación y una motivación reforzada.

9. ¿Cuál es su perspectiva sobre equilibrar (ponderar) la lesión de los derechos fundamentales del secreto e inviolabilidad de las comunicaciones con la neceesidad de investigar y esclarecer adecuadamente el delito de fraude informático?

Uno de los derechos fundamentales es la búsqueda de la verdad, por lo que consideramos que ante ponderar la lesión de los derechos fundamentales, estaría justificado ante la necesidad de la búsqueda de la verdad a través de la investigación y esclarecer adecuadamente el delito de Fraude Informático.

10. ¿Cuál es la evaluación general sobre el grado de lesividad de la medida restrictiva de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático, considerando los intereses del Estado y los derechos fundamentales de las personas involucradas?

Ningún derecho es absoluto, todos los derechos son relativos consideramos que debe primar el Derecho a la búsqueda de la verdad, dentro de la teoría de la ponderación según Robert Alexis señala que todos los Principios son derrotables, donde se debe primar los derechos de la colectividad ante el derecho individual de las

Personas.

11. ¿Considera usted que existen diferentes grados de lesión a los derechos fundamentales de los afectados respecto al levantamiento del secreto de las comunicaciones en sus formas de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica?

No, ya que sólo se afecta el derecho a la intimidad.

12. En su experiencia, ¿Existe alguna diferencia en los criterios que se utilizan para resolver requerimientos de levantamiento del secreto de las comunicaciones en su forma de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica, o se utiliza el mismo criterio?

Hasta el momento el criterio utilizado por el juez es el mismo, señalando y/o argumentado siempre sobre el derecho constitucional a la intimidad, a la inviolabilidad de las comunicaciones.

Mario Greco Orellana Cuadros
FISCAL PROVINCIAL (P)
Primera Fiscalía Provincial Penal
Corporativa - Huancayo

Firma y Sello

ANEXO 9. Cuestionario desarrollado por el fiscal provincial Luis Alvaro Cardenas Moreno.

Cuestionario

Título de la tesis: Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.

Nombres y Apellidos: Luis Alvaro Cardenas Moreno

Cargo: Fiscal Provincial

1. ¿Qué concepción tiene sobre el levantamiento del secreto de las comunicaciones?

es una medida limitativa de derecho que sirve para que operadores de justicia busquen información protegida por el derecho al secreto de las comunicaciones; actualmente es una medida utilizada frecuentemente en casos que revisten mayor complejidad, como podrían ser los delitos informáticos o de ciberdelincuencia.

2. ¿Qué concepción tiene sobre los delitos informáticos y el delito de fraude informático en particular?

Los delitos informáticos son todas aquellas conductas típicas, antijurídicas y culpables que se cometen en el soporte digital a través de las TIC (Tecnologías de la información y comunicación) en ese sentido el fraude informático es una modalidad de este tipo de delitos del tipo [illegible], porque el bien jurídico afectado es uno tradicional (el patrimonio) pero los medios son [illegible] de las TIC.

3. ¿Considera que el levantamiento del secreto de las comunicaciones es indispensable para las investigaciones en delitos informáticos?

Es [illegible] contar con esta medida limitativa de derechos, ya que sin ella sería casi imposible poder identificar al autor de los delitos y al [illegible] con los datos de [illegible] estar [illegible] con ellos.

4. En su experiencia: ¿Cómo afecta la exigencia del requisito de una sanción penal superior a cuatro años de pena privativa de libertad establecida en el numeral 1 del artículo 230 del Código Procesal Penal, para la autorización judicial de levantamiento de secreto de las comunicaciones en su forma de información histórica en los casos relacionados con el delito de fraude informático que conoció su despacho?

Bueno, inicialmente [illegible] L.S.C. [illegible] investigación [illegible] delito informático [illegible] 4 años [illegible] L.S.C.

5. ¿Cuáles son los criterios que se utiliza para aplicar el requisito de suma pena en la autorización judicial de levantamiento de secreto de las comunicaciones, con respecto a la pena establecida en el delito de fraude informático?

En realidad en los [illegible] artículo 238 [illegible] delitos informáticos [illegible] y lo más importante [illegible] L.S.C. para [illegible] a la defensa de estos delitos.

6. En su experiencia: ¿Ha observado algún impacto negativo en la investigación de delitos de fraude informático debido al posible rechazo de los requerimientos fiscales por no cumplir con el requisito de suma pena para el levantamiento del secreto de las comunicaciones?

Inicialmente sí, [illegible] por [illegible] que tienen [illegible] y [illegible] del LSC para el éxito de la investigación.

7. ¿Considera que el límite impuesto como presupuesto material de suma pena o prognosis de pena para el levantamiento del secreto de las comunicaciones en su forma de información histórica podría afectar la identificación y persecución de los responsables del delito de fraude informático?

Por lo visto creo que sí; es por ello que considero que dicho capítulo [illegible] a este tipo de delitos.

8. Respecto a la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional: ¿Considera que para la autorización judicial del levantamiento de secreto de las comunicaciones en los delitos informáticos aún se deba tener en cuenta los requisitos establecidos en dicha ley, o sólo el previsto en numeral 1 del artículo 230 del Código Penal, o ambas?

Actualmente lo que utilizamos es [illegible] en el inciso 1 del artículo 230 del CPP [illegible] suficiente para solicitar al juez [illegible] del LSC.

9. ¿Cuál es su perspectiva sobre equilibrar (ponderar) la lesión de los derechos fundamentales del secreto e inviolabilidad de las comunicaciones con la necesidad de investigar y esclarecer adecuadamente el delito de fraude informático?

Desde la perspectiva de la ponderación y la proporcionalidad de los [illegible] de [illegible] que es el LSC; [illegible] el LSC. En toda investigación por delitos informáticos es absolutamente necesario para salvaguardar los fines del proceso (esclarecimiento de los hechos y obtención de los medios de prueba), entonces el único mecanismo para la consecución de este objetivo es esta medida; por tanto es necesaria porque permitirá identificar a los presuntos autores o partícipes del hecho penal; respecto a la necesidad, no hay otra medida o [illegible] pueda obtener dicha solicitud; medida proporcional.

10. ¿Cuál es la evaluación general sobre el grado de lesividad de la medida restrictiva de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático, considerando los intereses del Estado y los derechos fundamentales de las personas involucradas?

Partiendo que este tipo delitos los bienes jurídicos protegidos son de diversa naturaleza, patrimonio, intimidad, propiedad intelectual, fe pública, etc. en donde el delito de fraude informático protege el patrimonio – que también resulta un derecho fundamental que es la propiedad la cual se ve vulnerada por el sujeto activo del delito; en tal sentido al hacer una ponderación entre el derecho afectado y la intervención que limitaría el derecho del investigado sobre su derecho constitucional de inviolabilidad del sec. de las comunicaciones consideramos que debe primar mayor preferencia y protección al fin supremo del Estado; aunado en estos tiempos en que esta actividad [illegible] se viene incrementando es más necesario dicha medida restrictiva

11. ¿Considera usted que existen diferentes grados de lesión a los derechos fundamentales de los afectados respecto al levantamiento del secreto de las comunicaciones en sus formas de intercepción de las comunicaciones en tiempo real, geolocalización e información histórica?

Es individual que existen grados de afectación en cuanto al tipo de USC. se requiere, por ejemplo la información histórica, es menos invasiva en cuanto a la intimidad y fuero de la comunicación y de todo ciudadano en relación a una intercepción de las comunicaciones en tiempo real, es por ello que el tipo de lesión o estos derechos fundamentales tendrían en correspondencia al tipo de delito investigado, por tanto, mientras mayor sea la lesión al este D° mayores tendrían que ser los justificaciones y necesidades para realizarlas.

12. En su experiencia, ¿Existe alguna diferencia en los criterios que se utilizan para resolver requerimientos de levantamiento del secreto de las comunicaciones en su forma de intercepción de las comunicaciones en tiempo real, geolocalización e información histórica, o se utiliza el mismo criterio?

Bueno, en cuanto a nuestra legislación el criterio utilizado para resolver este tipo de pedidos está regulado en el artículo 230° 1 del C.P., sin embargo, contrario a los señores jueces especialmente que tienen una interpretación errónea al respecto, que constituye una exigencia sine qua non para declarar fundado este pedido que se trata de delitos con penas superiores a cuatro años de PPL en su extremo mínimo cuando la norma no lo exige textualmente así.

Por otro lado, desde mi experiencia en la recopilación de información a la adquisición de pruebas electrónicas de proveedores de SS.UU. la relación al nivel de privacidad que otorga la ley al subscriptor, se indica que cuanto mas privacidad del carga legal del MP. no encontremos en los individuos, mayor será la requerimiento en este caso del

Firma y Sello

ANEXO 10. Cuestionario desarrollado por el fiscal provincial Elías Salcedo Ordaya.

Cuestionario

Título de la tesis: Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.

Nombres y Apellidos: Elías Salcedo ordaya

Cargo: Fiscal Provincial

1. ¿Qué concepción tiene sobre el levantamiento del secreto de las comunicaciones?

Es una medida coercitiva facultado al señor juez, quien previo requerimiento del fiscal ordena se levante el secreto de las comunicaciones, con la finalidad de lograr el exito de alguna investigación

2. ¿Qué concepción tiene sobre los delitos informáticos y el delito de fraude informático en particular?

Es un delito poco estudiado y tambien de dificil aplicacion por los conceptos en el campo tecnologico que no conocen los fiscales, jueces y abogados, lo cual implica capacitacion por unidades especializadas

3. ¿Considera que el levantamiento del secreto de las comunicaciones es indispensable para las investigaciones en delitos informáticos?

En algunos de ellos

4. En su experiencia: ¿Cómo afecta la exigencia del requisito de una sanción penal superior a cuatro años de pena privativa de libertad establecida en el numeral 1 del artículo 230 del Código Procesal Penal, para la autorización judicial de levantamiento de secreto de las comunicaciones en su forma de información histórica en los casos relacionados con el delito de fraude informático que conoció su despacho?

Que en muchos casos es el fundamento de los jueces para negar el requerimiento solicitado

5. ¿Cuáles son los criterios que se utiliza para aplicar el requisito de suma pena en la autorización judicial de levantamiento de secreto de las comunicaciones, con respecto a la pena establecida en el delito de fraude informático?

lo establecido en el codigo penal, con la aplicacion del sistema de tercios, lo cual no supera los 4 años cuando no tiene antecedentes, circunstancias agravantes

6. En su experiencia: ¿Ha observado algún impacto negativo en la investigación de delitos de fraude informático debido al posible rechazo de los requerimientos fiscales por no cumplir con el requisito de suma pena para el levantamiento del secreto de las comunicaciones?

Si se archivan los casos

7. ¿Considera que el límite impuesto como presupuesto material de suma pena o prognosis de pena para el levantamiento del secreto de las comunicaciones en su forma de información histórica podría afectar la identificación y persecución de los responsables del delito de fraude informático?

Si afecta

8. Respecto a la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional: ¿Considera que para la autorización judicial del levantamiento de secreto de las comunicaciones en los delitos informáticos aún se debe tener en cuenta los requisitos establecidos en dicha ley, o sólo el previsto en numeral 1 del artículo 230 del Código Penal, o ambas?

ya no porque el juez analiza el codigo penal

9. ¿Cuál es su perspectiva sobre equilibrar (ponderar) la lesión de los derechos fundamentales del secreto e inviolabilidad de las comunicaciones con la necesidad de investigar y esclarecer adecuadamente el delito de fraude informático?

Se debe aplicar el TEST de proporcionalidad

10. ¿Cuál es la evaluación general sobre el grado de lesividad de la medida restrictiva de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático, considerando los intereses del Estado y los derechos fundamentales de las personas involucradas?

No existe afectación a los intereses del grado la lesividad de la medida restrictiva, el Estado debe ser transparente en todo.

11. ¿Considera usted que existen diferentes grados de lesión a los derechos fundamentales de los afectados respecto al levantamiento del secreto de las comunicaciones en sus formas de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica?

que no, porque si es necesario debe levantarse el secreto

12. En su experiencia, ¿Existe alguna diferencia en los criterios que se utilizan para resolver requerimientos de levantamiento del secreto de las comunicaciones en su forma de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica, o se utiliza el mismo criterio?

Que no, pues cuando estamos ante un delito flagrante es necesario, pero cuando no existe esta causal si se vulnera Derechos Fundamentales

Firma y Sello

Elías Salcedo Ordaya
Fiscal Provincial
QUINTA FISCALÍA PROVINCIAL PENAL
CORPORATIVA DE HUANCAYO

ANEXO 11. Cuestionario desarrollado por el juez de investigación preparatoria Rafael Agustín Herrera Rivas

Cuestionario

Título de la tesis: Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.

Nombres y Apellidos: Rafael Agustín Herrera Rivas

Cargo: Juez del Primer Juzgado de Investigación Preparatoria de Huancayo

1. ¿Qué concepción tiene sobre el levantamiento del secreto de las comunicaciones?

La interceptación de las comunicaciones telefónicas supone una injerencia en el derecho fundamental de la persona investigada, que solo podría acordarse en el marco de una investigación penal con el fin de perseguir delitos graves y bajo siempre control jurisdiccional.

2. ¿Qué concepción tiene sobre los delitos informáticos y el delito de fraude informático en particular?

El delito informático, conocido también como delito cibernético o ciberdelito es toda acción antijurídica que se realiza en el entorno digital, espacio digital o de internet. Debido a la globalización digital de la sociedad, la delincuencia se ha expandido a esa dimensión. El fraude informático se encuentra previsto en el artículo 8 de la ley 30096 y se le imputa a aquel que a través de las tecnologías de la información o de la comunicación modifica un procedimiento.

3. ¿Considera que el levantamiento del secreto de las comunicaciones es indispensable para las investigaciones en delitos informáticos?

En algunos casos sí, en el que se requiere identificar al titular de la línea telefónica o cuentas electrónicas para viabilizar una investigación fiscal.

4. En su experiencia: ¿Cómo afecta la exigencia del requisito de una sanción penal superior a cuatro años de pena privativa de libertad establecida en el numeral 1 del artículo 230 del Código Procesal Penal, para la autorización judicial de levantamiento de secreto de las comunicaciones en su forma de información histórica en los casos relacionados con el delito de fraude informático que conoció su despacho?

La exigencia es para el Ministerio Público que no se satisfaga las expectativas de contar con dicha información, lo que dificulta las investigaciones por un tema de suma pena. art. 230 del CPP.

5. ¿Cuáles son los criterios que se utiliza para aplicar el requisito de suma pena en la autorización judicial de levantamiento de secreto de las comunicaciones, con respecto a la pena establecida en el delito de fraude informático?

Citando el artículo 230 del CPP., los pocos requerimientos fiscales que he tenido sobre levantamiento del secreto de las Comunicaciones, las he denegado por el tema de la SUMA PENA - dispo sición expresa de la ley procesal penal, ya que el delito de fraude informático establece un mínimo de 3 (tres) años.

6. En su experiencia: ¿Ha observado algún impacto negativo en la investigación de delitos de fraude informático debido al posible rechazo de los requerimientos fiscales por no cumplir con el requisito de suma pena para el levantamiento del secreto de las comunicaciones?

Bueno los señores fiscales no han apelado las denegatorias de sus requerimientos, pues entiendo que su denegatoria ha dificultado sus investigaciones por este delito de fraude informático.

7. ¿Considera que el límite impuesto como presupuesto material de suma pena o prognosis de pena para el levantamiento del secreto de las comunicaciones en su forma de información histórica podría afectar la identificación y persecución de los responsables del delito de fraude informático?

Considero que sí por lo que debe revisarse este aspecto legislativamente.

8. Respecto a la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional: ¿Considera que para la autorización judicial del levantamiento de secreto de las comunicaciones en los delitos informáticos aún se debe tener en cuenta los requisitos establecidos en dicha ley, o sólo el previsto en numeral 1 del artículo 230 del Código Penal, o ambas?

Dicha ley además contempla la excepción para delitos informáticos conforme al numeral 1 adicionado por la 3ª disp. Complementaria modificatoria de la ley Nº 30963 por lo si podría aplicarse (Principio de especialidad)

9. ¿Cuál es su perspectiva sobre equilibrar (ponderar) la lesión de los derechos fundamentales del secreto e inviolabilidad de las comunicaciones con la necesidad de investigar y esclarecer adecuadamente el delito de fraude informático?

Aplica el principio de proporcionalidad, a través del Subprincipio de proporcionalidad en sentido estricto consiste en aplicar la ley de ponderación donde la base a que cuenta mayor es el grado de la no satisfacción o de la afectación de un principio, tanto mayor tiene que ser la importancia de la satisfacción del otro".

10. ¿Cuál es la evaluación general sobre el grado de lesividad de la medida restrictiva de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático, considerando los intereses del Estado y los derechos fundamentales de las personas involucradas?

La lesividad está presente en cualquier caso si no dispone el levantamiento del secreto de las comunicaciones.

11. ¿Considera usted que existen diferentes grados de lesión a los derechos fundamentales de los afectados respecto al levantamiento del secreto de las comunicaciones en sus formas de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica?

Considero SI la afectación es UNICA y no puede diferenciarse en grados, es decir, no puede medirse.

12. En su experiencia, ¿Existe alguna diferencia en los criterios que se utilizan para resolver requerimientos de levantamiento del secreto de las comunicaciones en su forma de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica, o se utiliza el mismo criterio?

Hasta hace poco se tenía el mismo criterio de denegar el requerimiento cuando no satisfacía el requisito de la SERIA PENA, pero se viene variando dependiendo del caso en concreto y de conformidad a la ley 27697

RAFAEL AGUSTIN HERRERA RAMS
Juez
1° Juzgado de Investigación Preparatoria de Flagrancia
CORTE SUPERIOR DE JUSTICIA DE LIMA

Firma y Sello

ANEXO 12. Cuestionario desarrollado por el juez de investigación preparatoria Michael Henry Rojas Chancasanampa.

Cuestionario

Título de la tesis: Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.

Nombres y Apellidos: Michael Henry Rojas Chancasanampa

Cargo: Juez del Sexto Juzgado de Investigación Preparatoria de Huancayo

1. ¿Qué concepción tiene sobre el levantamiento del secreto de las comunicaciones?

El levantamiento del secreto de las comunicaciones es un medio especial de investigación, el cual consiste en obtener data del contenido de la misma manera que si este en concreto le asiste con la posibilidad de que la investigación obtenga pruebas (elemento de convicción), asimismo es una medida restrictiva al derecho fundamental del secreto de las comunicaciones, por lo que la medida debe ser tratada en cautela tomando en cuenta los requisitos procesales y el test de proporcionalidad.

2. ¿Qué concepción tiene sobre los delitos informáticos y el delito de fraude informático en particular?

Son conductas típicas, antijurídicas y culpables, en la que los sujetos típicos de ejecución informática para cometer delitos tradicionales, estos delitos se encuentran previstos en una ley especial - ley de delitos informáticos.

El delito de fraude informático es un delito contra el patrimonio en el que el sujeto activo hace uso de la tecnología con el fin de obtener un provecho económico ilícito.

3. ¿Considera que el levantamiento del secreto de las comunicaciones es indispensable para las investigaciones en delitos informáticos?

Considero que es indispensable para las investigaciones en delitos informáticos, pues por su naturaleza se requiere contar el uso de medios tecnológicos con el levantamiento de la misma para obtener datos que ayuden a identificar a los presuntos autores de delitos informáticos.

4. En su experiencia: ¿Cómo afecta la exigencia del requisito de una sanción penal superior a cuatro años de pena privativa de libertad establecida en el numeral 1 del artículo 230 del Código Procesal Penal, para la autorización judicial de levantamiento de secreto de las comunicaciones en su forma de información histórica en los casos relacionados con el delito de fraude informático que conoció su despacho?

Es una limitante para la investigación por parte del Ministerio Público, pues no pueden o no tienen otro medio para poder llegar a los posibles autores del delito de fraude informático, siendo la pena el limitante la autorización judicial en la que se deben de tener en cuenta los criterios de los requisitos previos contenidos en el artículo 230 del Código Penal.

5. ¿Cuáles son los criterios que se utiliza para aplicar el requisito de suma pena en la autorización judicial de levantamiento de secreto de las comunicaciones, con respecto a la pena establecida en el delito de fraude informático?

Los criterios que se toman en cuenta para autorizar el levantamiento del secreto de las comunicaciones son los establecidos en el artículo 230.1 del Código Procesal Penal, esto ya necesidad de la medida, siguientes elementos de convicción y que exista la pena de 4 años o una pluralidad de hechos y que deben tener en cuenta el test de proporcionalidad

6. En su experiencia: ¿Ha observado algún impacto negativo en la investigación de delitos de fraude informático debido al posible rechazo de los requerimientos fiscales por no cumplir con el requisito de suma pena para el levantamiento del secreto de las comunicaciones?

Los representantes del Ministerio Público en casos de delitos informáticos en los que requieren levantamiento del secreto de las comunicaciones y estos fueron rechazados no fueron apelados, esto por lo que estaremos que se archiven por no conseguir elementos de convicción que sustenten su caso.

7. ¿Considera que el límite impuesto como presupuesto material de suma pena o prognosis de pena para el levantamiento del secreto de las comunicaciones en su forma de información histórica podría afectar la identificación y persecución de los responsables del delito de fraude informático?

Considero que el límite impuesto por el Código Procesal Penal como requisito para el afecte la investigación y persecución de

delito de fraude informático y el no poder identificar a los posibles autores se crea impunidad ante este tipo de delitos.

8. Respecto a la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional: ¿Considera que para la autorización judicial del levantamiento de secreto de las comunicaciones en los delitos informáticos aún se debe tener en cuenta los requisitos establecidos en dicha ley, o sólo el previsto en numeral 1 del artículo 230 del Código Penal, o ambas?

Dicha ley otorga un beneficio en la que se excluye el 2 de los requisitos del Código Procesal Penal, aunque se debería aplicar por el criterio del principio de especialidad.

9. ¿Cuál es su perspectiva sobre equilibrar (ponderar) la lesión de los derechos fundamentales del secreto e inviolabilidad de las comunicaciones con la necesidad de investigar y esclarecer adecuadamente el delito de fraude informático?

El necesario equilibrio a ponderar la lesión con el objetivo de la restricción del derecho, es decir no podemos sacrificar un derecho fundamental como el secreto a las comunicaciones cuando el objetivo de la misma no contenga la adecuada necesidad de requerirlo en la investigación.

10. ¿Cuál es la evaluación general sobre el grado de lesividad de la medida restrictiva de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático, considerando los intereses del Estado y los derechos fundamentales de las personas involucradas?

La ponderación general entre los intereses del Estado y los derechos fundamentales de las personas a los que se les intervienen las comunicaciones y telecomunicaciones se encuentran sujetos bajo el texto de proporcionalidad, por lo que, de esta manera se podrá ver si la investigación se requiere necesariamente levantar el secreto de las comunicaciones para esclarecer los hechos. En este sentido se debe tener en cuenta el principio de la intervención de las comunicaciones y la lesión del derecho fundamental debe ser proporcional.

11. ¿Considera usted que existen diferentes grados de lesión a los derechos fundamentales de los afectados respecto al levantamiento del secreto de las comunicaciones en sus formas de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica?

Considero que si existen diferentes grados de lesión a los derechos fundamentales cuando estos faltan de estar en los que se requieren información histórica, intercepción en tiempo real y geolocalización ; pues no es lo mismo que mediante la intercepción en tiempo real se escuchen conversaciones privadas entre personas, lo cual tiene mayor lesión al derecho vulnerado, que cuando en los casos en los que se requieren información histórica la cual sea menor la lesión por ser menos intrusiva.

12. En su experiencia, ¿Existe alguna diferencia en los criterios que se utilizan para resolver requerimientos de levantamiento del secreto de las comunicaciones en su forma de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica, o se utiliza el mismo criterio?

En mi experiencia no existe diferencia en los criterios utilizados para resolver la autorización de levantamiento del secreto de las comunicaciones en tiempo real, geolocalización o información histórica pues la legislación establece los requisitos para su autorización y no diferencia unos de otros a pesar que en la practica se evidencia la necesidad de diferenciarlos, por lo que el criterio utilizado en estos casos es el mismo.

Firma y Sello

ANEXO 13. Cuestionario desarrollado por el juez de investigación preparatoria

Segundo Juan Huamán Carrasco

Cuestionario

Titulo de la tesis: Levantamiento del secreto de las comunicaciones en su forma de información histórica en el delito de fraude informático.

Nombres y Apellidos: Segundo Juan Huamán Carrasco

Cargo: Juez del Séptimo Juzgado de Investigación Preparatoria de Huancayo

1. ¿Qué concepción tiene sobre el levantamiento del secreto de las comunicaciones?

Constituye la orden impartida por el Juez de Investigación Preparatoria previo requerimiento fiscal debidamente motivado, a fin de que las operadoras de telefonía brinden información histórica respecto de las comunicaciones realizadas y recepcionadas por un imputado con sus (Imputados, familiares o terceros, a fin de obtener información para el esclarecimiento de los hechos que se investiga

2. ¿Qué concepción tiene sobre los delitos informáticos y el delito de fraude informático en particular?

El delito informático es la acción ilegal, delictiva que hacen uso de dispositivos electrónicos e internet a fin de vulnerar, amenazar o dañar bienes patrimoniales o no, de personas o entidades públicas o privadas.

Considero que el delito de fraude informático es el comportamiento que afecta el software o soporte lógico de un sistema automatizado de la información.

3. ¿Considera que el levantamiento del secreto de las comunicaciones es indispensable para las investigaciones en delitos informáticos?

Considero que si es importante el levantamiento del Secreto de las comunicaciones en la investigación de los delitos informáticos, a fin de que exista una tutela efectiva de los bienes jurídicos de este tipo de delitos debido a que permitirá identificar al titular de la acción u obtener indicios de la identidad del autor.

4. En su experiencia: ¿Cómo afecta la exigencia del requisito de una sanción penal superior a cuatro años de pena privativa de libertad establecida en el numeral 1 del artículo 230 del Código Procesal Penal, para la autorización judicial de levantamiento de secreto de las comunicaciones en su forma de información histórica en los casos relacionados con el delito de fraude informático que conoció su despacho?

Efectivamente constituye un problema en la investigación fiscal en este tipo de delitos debido a las limitadas herramientas de investigación en este tipo de delitos, siendo la principal limitación la autorización solicitada a los jueces para poder realizar el levantamiento del secreto de las comunicaciones, obteniendo denegatorias por no cumplir los presupuestos del art. 230 C.P.P. que en el delito debe tener una pena no menor de 4 años de PPL, dificultando la investigación para identificar al imputado paralizando el archivo.

5. ¿Cuáles son los criterios que se utiliza para aplicar el requisito de suma pena en la autorización judicial de levantamiento de secreto de las comunicaciones, con respecto a la pena establecida en el delito de fraude informático?

El levantamiento del secreto de las comunicaciones procederá cuando se cumplan con los presupuestos de la medida, siendo esta requerida debidamente fundamentada en el requerimiento fiscal, debidamente sustentada con suficientes elementos de convicción y esta medida según la norma antes citada procede en las investigaciones de delitos con pena superior a los 4 años y además debe superar el principio de proporcionalidad.

6. En su experiencia: ¿Ha observado algún impacto negativo en la investigación de delitos de fraude informático debido al posible rechazo de los requerimientos fiscales por no cumplir con el requisito de suma pena para el levantamiento del secreto de las comunicaciones?

Durante mi experiencia no se ha requerido por parte del Ministerio Público el levantamiento del Secreto de la Comunicaciones en delitos de fraude informático, además de ser muy poco los investigaciones por este tipo de delitos.

7. ¿Considera que el límite impuesto como presupuesto material de suma pena o prognosis de pena para el levantamiento del secreto de las comunicaciones en su forma de información histórica podría afectar la identificación y persecución de los responsables del delito de fraude informático?

Teniendo en cuenta que este tipo de delitos en el mundo contemporáneo tienden a incrementarse

considero que a fin de que no queden impunes este tipo de delitos (fraude informático) debe concederse el levantamiento del Secreto de las Comunicaciones a fin de obtener la prueba a fin de que el fiscal pueda recabar los elementos de convicción suficientes que acrediten el ilícito penal, claro está sin vulnerar los límites que la norma establece.

8. Respecto a la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional: ¿Considera que para la autorización judicial del levantamiento de secreto de las comunicaciones en los delitos informáticos aún se debe tener en cuenta los requisitos establecidos en dicha ley, o sólo el previsto en numeral 1 del artículo 230 del Código Penal, o ambas?

En primer lugar debemos tener presente la jerarquía de normas, así tenemos por un lado el artículo 230 inciso 1 del Código Procesal Penal y por otro lado la ley N° 27697 por lo que debe prevalecer el Código Procesal Penal, sin embargo, se puede conceder autorización para el LSC de manera excepcional, siempre y cuando el Fiscal lo solicite mediante requerimiento debidamente motivado, acompañado de suficiente elementos de convicción.

9. ¿Cuál es su perspectiva sobre equilibrar (ponderar) la lesión de los derechos fundamentales del secreto e inviolabilidad de las comunicaciones con la necesidad de investigar y esclarecer adecuadamente el delito de fraude informático?

La ponderación se realiza al momento de expedir la resolución de autorización del levantamiento del secreto de las comunicaciones y esto obedece a que se cumpla con los requisitos para su concesión, entre estos requisitos encontramos el principio de proporcionalidad de la medida, el mismo que se subdivide en 3 subprincipios: idoneidad, necesidad y proporcionalidad en sentido estricto. En tal sentido deberá ponderarse el derecho que tiene el imputado y el bien jurídico protegido.

10. ¿Cuál es la evaluación general sobre el grado de lesividad de la medida restrictiva de levantamiento del secreto de las comunicaciones en su forma de información histórica en la investigación de delitos de fraude informático, considerando los intereses del Estado y los derechos fundamentales de las personas involucradas?

En primer lugar debemos precisar que el principio de lesividad viene ha ser la exclusiva protección de bienes jurídicos y como principio de ofensividad y como una expresión de una efectiva puesta en peligro o ser un bien jurídico específico, siendo así corresponde efectuar una ponderación si el derecho constitucional del secreto de las comunicaciones que goza toda persona

resulta necesario o no para proteger el bien jurídico, pero en el caso particular para que proceda el LSC la investigación debe ser compleja y por ende sea imprescindible el LSC.

11. ¿Considera usted que existen diferentes grados de lesión a los derechos fundamentales de los afectados respecto al levantamiento del secreto de las comunicaciones en sus formas de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica?

Considero que si existen diferentes grados, es por ello que se debe tener en cuenta los principios de razonabilidad y proporcionalidad de la medida, realizando la ponderación entre el derecho a afectar (LSC) y la investigación y riesgos y cuando sea el único medio para esclarecer los hechos, pues si existe otro elemento de convicción que acredite los hechos estaría demás ordenar el LSC. esto quiere decir, que no en todos casos puede ordenarse el LSC, sino únicamente en investigaciones complejidad de agentes etc.

12. En su experiencia, ¿Existe alguna diferencia en los criterios que se utilizan para resolver requerimientos de levantamiento del secreto de las comunicaciones en su forma de interceptación de las comunicaciones en tiempo real, geolocalización e información histórica, o se utiliza el mismo criterio?

Para conceder el LSC y la intercepción de las comunicaciones se tienen en cuenta los mismos criterios ya antes tienen que ver con derechos fundamentales reconocidos en la Constitución Política del Estado, asimismo el fiscal al solicitar el LSC, también solicita la intercepción de las comunicaciones en tiempo real, geolocalización e información histórica, dado este respecto de otros delitos cuyas penas superan los 4 años de PPL.

SEGUNDO J. HUAMAN CARRASCO
Juez (T)
Juzgado de Investigación Preparatoria de Huancayo
CORTE SUPERIOR DE JUSTICIA DE JUNIN

Firma y Sello