Universidad Continental

FACULTAD DE DERECHO

Escuela Académico Profesional de Derecho

Tesis

La aplicación de la incautación de bienes en el delito informático *Sim Swapping*

Brighite Sarela Malaga Pinto
Yaritza Mercedes Pinto Bejarano
Daniela Ines Rodriguez Condori

Para optar el Título Profesional de Abogado

Huancayo, 2023

Universidad Continental

INFORME DE CONFORMIDAD DE ORIGINALIDAD DE TESIS

A	**:**	Eliana Mory Arciniega Decano de la Facultad de Derecho
DE	**:**	Héctor Fidel Rojas Rodríguez Asesor de tesis
ASUNTO	**:**	Remito resultado de evaluación de originalidad de tesis
FECHA	**:**	5 de diciembre de 2023

Con sumo agrado me dirijo a vuestro despacho para saludarla en calidad de asesor de la tesis titulada: "**LA APLICACIÓN DE LA INCAUTACIÓN DE BIENES EN EL DELITO INFORMÁTICO *SIM SWAPPING***", perteneciente a las estudiantes **Malaga Pinto, Brighite Sarela; Pinto Bejarano Yaritza Mercedes y Rodriguez Condori, Daniela Ines**, de la E.A.P. de Derecho; al respecto le informo que se procedió a cargar el documento de tesis en la plataforma "Turnitin" y se realizó la verificación completa de las coincidencias resaltadas por el software, dando por resultado 20 % de similitud (informe adjunto) 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 (Nº de palabras excluidas: 10) SI [X] NO [ ]
- Exclusión de fuente por trabajo anterior del mismo estudiante SI [ ] NO [X]

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

Recae toda responsabilidad del contenido de la tesis sobre el autor y asesor, en concordancia a los principios de legalidad, presunción de veracidad y simplicidad, expresados en el Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales – RENATI y en la Directiva 003-2016-R/UC.

Esperando la atención a la presente, me despido sin otro particular y sea propicia la ocasión para renovar las muestras de mi especial consideración.

Atentamente,

Héctor Fidel Rojas Rodríguez
Asesor de tesis

Cc.
Facultad
Oficina de Grados y Títulos
Interesado(a)

DECLARACIÓN JURADA DE AUTENTICIDAD

Yo, Daniela Ines Rodriguez Condori, identificado(a) con Documento Nacional de Identidad No. 76256468, de la E.A.P. de Derecho de la Facultad de Derecho la Universidad Continental, declaro bajo juramento lo siguiente:

1. La tesis titulada: "LA APLICACIÓN DE LA INCAUTACIÓN DE BIENES EN EL DELITO INFORMÁTICO *SIM SWAPPING*", es de mi autoría, la misma que presento para optar el Título Profesional de Abogado.
2. La tesis no ha sido plagiada 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. La tesis es original e inédita, 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, asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a las acciones legales pertinentes.

04 de Diciembre de 2023.

Daniela Ines Rodriguez Condori

DNI. No. 76256468

Cc.
Facultad
Oficina de Grados y Títulos
Interesado(a)

DECLARACIÓN JURADA DE AUTENTICIDAD

Yo, Yaritza Mercedes Pinto Bejarano, identificado(a) con Documento Nacional de Identidad No. 70581845, de la E.A.P. de Derecho de la Facultad de Derecho la Universidad Continental, declaro bajo juramento lo siguiente:

1. La tesis titulada: "LA APLICACIÓN DE LA INCAUTACIÓN DE BIENES EN EL DELITO INFORMÁTICO *SIM SWAPPING*", es de mi autoría, la misma que presento para optar el Título Profesional de Abogado.
2. La tesis no ha sido plagiada 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. La tesis es original e inédita, 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, asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a las acciones legales pertinentes.

04 de Diciembre de 2023.

YARITZA MERCEDES PINTO BEJARANO

DNI. No. 70581845

Cc.
Facultad
Oficina de Grados y Títulos
Interesado(a)

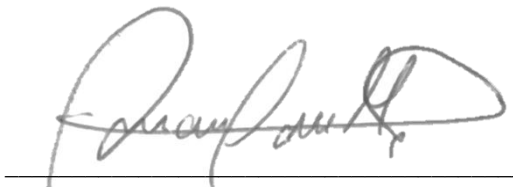
DECLARACIÓN JURADA DE AUTENTICIDAD

Yo, Brighite Sarela Malaga Pinto, identificado(a) con Documento Nacional de Identidad No. 71573122 de la E.A.P. de Derecho de la Facultad de Derecho la Universidad Continental, declaro bajo juramento lo siguiente:

1. La tesis titulada: "LA APLICACIÓN DE LA INCAUTACIÓN DE BIENES EN EL DELITO INFORMÁTICO *SIM SWAPPING* ", es de mi autoría, la misma que presento para optar el Título Profesional de Abogado.
2. La tesis no ha sido plagiada 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. La tesis es original e inédita, 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, asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a las acciones legales pertinentes.

04 de Diciembre de 2023.



Brighite Sarela Málaga Pinto

DNI. No. 71573122

Cc.
Facultad
Oficina de Grados y Títulos
Interesado(a)

sim swapping

INFORME DE ORIGINALIDAD

20%	20%	4%	9%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.ucv.edu.pe Fuente de Internet	2%
2	qdoc.tips Fuente de Internet	2%
3	hdl.handle.net Fuente de Internet	2%
4	idoc.pub Fuente de Internet	1%
5	repositorio.unsa.edu.pe Fuente de Internet	1%
6	repositorio.uap.edu.pe Fuente de Internet	1%
7	repositorio.uchile.cl Fuente de Internet	<1%
8	www.scribd.com Fuente de Internet	<1%
9	Submitted to Pontificia Universidad Catolica del Peru	<1%

Trabajo del estudiante

10	livrosdeamor.com.br Fuente de Internet	<1 %
11	issuu.com Fuente de Internet	<1 %
12	www.dspace.uce.edu.ec Fuente de Internet	<1 %
13	repositorio.pucp.edu.pe Fuente de Internet	<1 %
14	revistas.pucp.edu.pe Fuente de Internet	<1 %
15	vsip.info Fuente de Internet	<1 %
16	repositorio.uns.edu.pe Fuente de Internet	<1 %
17	rio.upo.es Fuente de Internet	<1 %
18	www.dialogoconlajurisprudencia.com Fuente de Internet	<1 %
19	www.defensoria.gob.pe Fuente de Internet	<1 %
20	www.slideshare.net Fuente de Internet	<1 %
21	Submitted to Universidad Católica San Pablo	

	Trabajo del estudiante	<1 %
22	docplayer.es Fuente de Internet	<1 %
23	repository.javeriana.edu.co Fuente de Internet	<1 %
24	Submitted to Universidad Continental Trabajo del estudiante	<1 %
25	www.enfoquederecho.com Fuente de Internet	<1 %
26	prezi.com Fuente de Internet	<1 %
27	coe.int Fuente de Internet	<1 %
28	revistas.pj.gob.pe Fuente de Internet	<1 %
29	Submitted to Universidad San Ignacio de Loyola Trabajo del estudiante	<1 %
30	doku.pub Fuente de Internet	<1 %
31	enestrado.com Fuente de Internet	<1 %
32	repositorio.uss.edu.pe Fuente de Internet	

		<1 %
33	derecho.udd.cl Fuente de Internet	<1 %
34	www.gob.pe Fuente de Internet	<1 %
35	revistas.ulima.edu.pe Fuente de Internet	<1 %
36	www.ccd.com.co Fuente de Internet	<1 %
37	Submitted to Universidad Señor de Sipan Trabajo del estudiante	<1 %
38	Submitted to IPChile Trabajo del estudiante	<1 %
39	Submitted to Universidad Tecnologica del Peru Trabajo del estudiante	<1 %
40	repositorio.unp.edu.pe Fuente de Internet	<1 %
41	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1 %
42	dspace.unitru.edu.pe Fuente de Internet	<1 %
43	www.suin-juriscol.gov.co Fuente de Internet	

		<1 %
44	repositorio.unjfsc.edu.pe Fuente de Internet	<1 %
45	es.scribd.com Fuente de Internet	<1 %
46	lpderecho.pe Fuente de Internet	<1 %
47	cdn.www.gob.pe Fuente de Internet	<1 %
48	marizavt92.wordpress.com Fuente de Internet	<1 %
49	repositorio.ulasamericas.edu.pe Fuente de Internet	<1 %
50	repositorio.unheval.edu.pe Fuente de Internet	<1 %
51	repositorio.usil.edu.pe Fuente de Internet	<1 %
52	Submitted to Universidad de Lima Trabajo del estudiante	<1 %
53	www.congreso.gob.pe Fuente de Internet	<1 %
54	www.produccioncientificaluz.org Fuente de Internet	<1 %

55	www.tuabogadodefensor.com Fuente de Internet	<1 %
56	dokumen.site Fuente de Internet	<1 %
57	es.slideshare.net Fuente de Internet	<1 %
58	www.bcn.cl Fuente de Internet	<1 %
59	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 36 (2020) (VOLUME II)", Brill, 2022 Publicación	<1 %
60	prcp.com.pe Fuente de Internet	<1 %
61	www.mpfn.gob.pe Fuente de Internet	<1 %
62	documentop.com Fuente de Internet	<1 %
63	José Antonio Caro John, José Leandro Reaño Peschiera. "Responsabilidad penal de la empresa y criminal compliance. Aspectos sustantivos y procesales", Forseti: Revista de Derecho, 2022 Publicación	<1 %

64	repositorio.usmp.edu.pe Fuente de Internet	<1 %
65	www.sic.gov.co Fuente de Internet	<1 %
66	repositorio.une.edu.pe Fuente de Internet	<1 %
67	angelderechoinformatico.blogspot.com Fuente de Internet	<1 %
68	repositorio.unfv.edu.pe Fuente de Internet	<1 %
69	www.coursehero.com Fuente de Internet	<1 %
70	www.cej-mjusticia.es Fuente de Internet	<1 %
71	aaspsite.blob.core.windows.net Fuente de Internet	<1 %
72	estudioderechoylibertad.com Fuente de Internet	<1 %
73	repositorio.upla.edu.pe Fuente de Internet	<1 %
74	www.sbs.gob.pe Fuente de Internet	<1 %
75	1library.co Fuente de Internet	<1 %

76	Submitted to CONACYT Trabajo del estudiante	<1 %
77	repositorio.upagu.edu.pe Fuente de Internet	<1 %
78	derecho.unap.edu.pe Fuente de Internet	<1 %
79	fundacion-rama.com Fuente de Internet	<1 %
80	repositorio.autonomadeica.edu.pe Fuente de Internet	<1 %
81	Submitted to Corporación Universitaria Minuto de Dios, UNIMINUTO Trabajo del estudiante	<1 %
82	Submitted to Escuela de Posgrado PNP Trabajo del estudiante	<1 %
83	Submitted to Universidad Catolica Los Angeles de Chimbote Trabajo del estudiante	<1 %
84	Submitted to Universidad Rey Juan Carlos Trabajo del estudiante	<1 %
85	bibliotecavirtual.dgb.umich.mx:8083 Fuente de Internet	<1 %
86	docentegrimaldochong11.blogspot.com Fuente de Internet	<1 %

87	repositorio.unprg.edu.pe Fuente de Internet	<1 %
88	revistainstitucional.amag.edu.pe Fuente de Internet	<1 %
89	www.cingular.net Fuente de Internet	<1 %
90	Submitted to Universidad de San Martín de Porres Trabajo del estudiante	<1 %
91	epdf.pub Fuente de Internet	<1 %
92	html.rincondelvago.com Fuente de Internet	<1 %
93	sil.gobernacion.gob.mx Fuente de Internet	<1 %
94	www.dspace.unitru.edu.pe Fuente de Internet	<1 %
95	www.pdhumanos.org Fuente de Internet	<1 %
96	www.researchgate.net Fuente de Internet	<1 %
97	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 23 (2007)", Brill, 2012 Publicación	<1 %

98	buscador.eluniversal.com Fuente de Internet	<1 %
99	curanderasguatemala.home.blog Fuente de Internet	<1 %
100	docta.ucm.es Fuente de Internet	<1 %
101	kupdf.net Fuente de Internet	<1 %
102	repositorio.unasam.edu.pe Fuente de Internet	<1 %
103	revistas.urp.edu.pe Fuente de Internet	<1 %
104	scm.oas.org Fuente de Internet	<1 %
105	www.grafiati.com Fuente de Internet	<1 %
106	www.poe.org.ar Fuente de Internet	<1 %
107	xdocs.net Fuente de Internet	<1 %

Excluir citas	Activo	Excluir coincidencias	< 10 words
Excluir bibliografía	Activo		

DEDICATORIA

El presente trabajo va dedicado a Dios por darnos la fuerza y voluntad para guiar nuestras vidas por el camino correcto para cumplir nuestras metas tanto personales como profesionales.

A nuestros padres, por darnos el privilegio de la educación y brindarnos constantemente su apoyo incondicional a lo largo de este proceso de preparación.

AGRADECIMIENTOS

A nuestros padres por impulsarnos a tener perseverancia para concluir nuestras metas.

Asimismo, queremos expresar un agradecimiento sincero a nuestro asesor, Mg. Héctor Fidel Rojas Rodriguez, por su paciencia, dedicación y orientación en la realización del trabajo de investigación.

Finalmente, es necesario agradecer a la Universidad Continental, por acogernos y permitirnos ser parte de esta familia.

RESUMEN

Las nuevas tecnologías de información y comunicación, adoptadas por el hombre en sus actividades de desarrollo, conllevan nuevas modalidades de comisión de delitos a través de medios informáticos y cibernéticos. Esto implica que los fraudes con consecuencias económicas o patrimoniales no necesariamente deben tener como objeto de la acción delictiva a bienes corpóreos, sino que la delincuencia informática realiza el apoderamiento del patrimonio de sus víctimas mediante herramientas informáticas. En ese orden de ideas, la presente investigación tiene como como objetivo analizar la aplicabilidad de la incautación como medida instrumental del proceso penal inicialmente diseñada para la aprehensión física de bienes corpóreos a una figura específica del delito informático denominada *SIM swapping.* Una utilización de este tipo permitiría la investigación más eficiente de este tipo de criminalidad al no requerirse el extremo formalismo que se puede apreciar en el caso del levantamiento del secreto bancario, que es la medida de búsqueda de pruebas que se entiende como" idónea" para enfrentar estos casos.

A través del análisis dogmático, el trabajo concluye en la efectividad de la aplicación de la incautación de bienes como medida instrumental regulada en el proceso penal al delito de *SIM swapping*, ya que es un mecanismo procesal viable y que encuentra respaldo en el derecho comparado.

Palabras clave: *SIM swapping*, delito informativo, ciberdelincuencia, sociedad de la información, incautación, levantamiento del secreto bancario.

ABSTRACT

The new information and communication technologies, adopted by people in their development activities, involve new modalities of committing crimes through computer and cyber media. This implies that frauds with economic or patrimonial consequences should not necessarily have tangible property as the object of the criminal action, but that computer crime seizes the patrimony of its victims through computer tools. In this order of ideas, the present research has as purpose to analyze the applicability of the seizure as an instrumental measure of the criminal process initially designed for the physical apprehension of tangible assets to a specific figure of computer crime called *SIM swapping*. A use of this type would allow the most efficient research of this type of crime by not requiring the extreme formalism that can be seen in the case of the lifting of bank secrecy, which is the measure of search for evidence that is understood as "suitable" for deal with these cases.

Through dogmatic analysis, the research paper concludes on the effectiveness of the application of the seizure of assets as an instrumental measure regulated in the criminal process to the crime of *SIM swapping,* since it is a viable procedural mechanism that finds support in comparative law.

Keywords: *SIM swapping*, information crime, cybercrime, information society, seizure, lifting of bank secrecy.

ÍNDICE

ÍNDICE DE TABLA

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La irrupción de las tecnologías de la información ha conllevado la discusión respecto a la efectividad de las figuras jurídicas clásicas y la necesidad de su adaptación a los nuevos tiempos. De esta controversia no es ajeno el derecho penal aplicado, campo en el cual se discute la utilidad de las figuras delictivas clásicas para combatir atentados contra bienes jurídicos relevantes socialmente mediante nuevas modalidades delictivas. Tal es el caso de delito informático de *SIM swapping*, donde se denota que la medida procesal de levantamiento del secreto bancario, cuya finalidad es recabar indicios de ilícitos vinculados con la intromisión en las cuentas bancarias de la víctima a través del uso de mecanismos informáticos de intromisión o de la utilización de cuentas bancarias de terceros, se ve inutilizada por los excesivos plazos para su concesión, en comparación con la velocidad a la que pueden desaparecer los rastros del delito con que se cometen dichos atentados. En tal contexto, surge la interrogante de si es verdaderamente esta medida procesal limitativa de derechos la idónea para la recolección de indicios que aporten a una investigación efectiva frente a este tipo de delitos.

La incautación es una media de coerción patrimonial que tiene una composición jurídica dual: como medida de búsqueda de prueba y de restricción de derechos, y como medida de coerción. Por lo que podemos sostener que la institución procesal de la incautación es una perfecta alternativa aplicable a este delito, a fin de proporcionar una persecución efectiva y eficiente a este delito, se obtiene mejores resultados en el extremo de que hay una adecuada ubicación y preservación de la prueba, pues resulta más rápida en su accionar, lo cual garantiza su conservación (custodia) y su llegada de juicio oral. Por ello, la propuesta interpretativa aquí defendida es que debe recurrirse a la incautación en los delitos informáticos, más aún cuando se trate del delito de *SIM swapping*, ya que como se expuso previamente, la naturaleza de este tipo penal permite la manipulación de la información

(datos y/o sistemas informáticos), proporcionándole al autor del delito la facilidad de poder extinguir o manipular la prueba, si es que no se aplica un tratamiento correcto en la etapa de investigación preparatoria.

Para el desarrollo de esta investigación se han planteado cuatro capítulos. En el primero de ellos se consigna los aspectos metodológicos del trabajo.

En el capítulo 2, se expone el estado situacional (estado del arte) del tipo penal de fraude informático *SIM swapping* en el Perú, evidenciando que se trata de una figura novedosa en el ordenamiento jurídico nacional; tras su análisis, se desprende que se trata de un delito que vulnera el patrimonio, por medio de la manipulación de datos y/o sistemas informáticos, que causa un perjuicio económico al titular.

En el capítulo 3, se desarrolla el marco teórico de la propuesta de solución planteada como base de la investigación; para lo cual se analiza los alcances de la analogía en derecho penal y, en particular, de la posibilidad de aplicar dicho método interpretativo cuando ello resulta favorable al reo; asimismo se revisa el marco internacional compuesto principalmente por el Convenio de Budapest, como eje normativo para señalar que siendo el Perú un Estado parte del referido convenio, tiene como obligación internacional garantizar las medidas procesales para combatir la ciberdelincuencia. Asimismo, siendo que ya desde un plano normativo constitucional, el Estado peruano tutela los derechos individuales en relación con los datos informáticos (art. 2.6 de la Constitución), ante la ocurrencia de eventos que vulneren los mismos, está obligado a sancionar tales conductas ilícitas.

Con estas bases teóricas, la presente investigación demuestra en el capítulo 4 (verificación de la hipótesis) que es viable la aplicación de la medida procesal de incautación en los casos de comisión del delito informático *SIM swapping*, utilizando para ello la analogía como método de integración de las normas jurídicas, sin que ello signifique afectar los derechos del imputado. Esta conclusión general se fundamenta en un análisis de carácter

estrictamente dogmático; desprendiéndose del mismo que, si bien es cierto la medida del levantamiento del secreto bancario regulada en el artículo 235 inciso 1 del Código Procesal Penal (2004) tiene como fin recolectar elementos de convicción para la comprobación de los hechos constitutivos de delitos informáticos, esta no es la única medida para tal fin. Puesto que, ante los excesivos plazos para su ejecución, es válido recurrir, como alternativa con mayor eficacia, a la incautación de bienes, teniendo como principal eje los datos y sistemas informáticos, dándose la posibilidad de que efectivamente esta medida procesal se aplique en nuestra legislación, todo ello con la finalidad de garantizar la persecución del delito.

CAPÍTULO I

ASPECTOS METODOLÓGICOS

1.1. Tema Delimitado

La medida de incautación de bienes en el delito informático denominado *SIM swapping.*

1.2. Problema de Investigación

¿Se puede aplicar la incautación de bienes al delito informático del *SIM swapping*?

1.3. Objetivos

1.3.1. Objetivo general

Analizar la aplicabilidad de la incautación de bienes, como medida instrumental regulada en el proceso penal, al delito informático *SIM swapping.*

1.3.2. Objetivos específicos

- Identificar si el levantamiento del secreto bancario es una figura procesal limitativa de derechos suficiente para responder a la problemática de los delitos informáticos.
- Analizar si la norma procesal puede aplicarse por analogía favorable al imputado en el caso del delito informático *SIM swapping.*

1.4. Hipótesis

La aparición del Internet y su impacto en la vida cotidiana de las personas conlleva, sin duda, al avance progresivo de la tecnología en nuestras vidas, lo que al mismo tiempo nos permite *SIM*plificar y optimizar ciertas actividades frecuentes dentro del medio en el que

nos desarrollamos; por ejemplo, las compras *online*, que significan un verdadero apoyo para nuestra sociedad, o el pago de servicios desde aplicativos u otros *SIM*ilares, lo que permite *SIM*plificar el trámite.

Bajo esta premisa, podemos denotar algunos de los múltiples beneficios que resultan de la aplicación de estas tecnologías, sin embargo, y no siendo menos importante este nuevo medio cibernético generado en el que venimos interactuando, genera la intervención de intrusos con fines delictivos en la *web*, lo que da como resultado la aparición de nuevas modalidades de delinquir a través de medios tecnológicos; dentro de ellos, la más inusual, por su *modus operandi*, es el denominado *SIM swapping* o suplantación de chip.

El *SIM swapping* implica en suplantar la tarjeta *SIM* del móvil, logrando la recopilación de información personal que es almacenada en dicho equipo. Para tal efecto, los perpetradores logran apropiarse de los datos del titular de la línea telefónica (por ejemplo, su número de cuenta bancaria y clave de acceso) a través del *phishing* (uso de aplicaciones fraudulentas), el envío de señales de wifi falsas, entre otras modalidades.

Ante esta conducta ilícita, los medios con los que cuenta nuestro ordenamiento jurídico y los titulares de ejercer la acción penal para obtener la información que permita identificar a los presuntos autores del delito, ya sea buscándola en el sistema bancario, en las bases de datos de las empresas de telecomunicación, toma un excesivo tiempo en obtenerse; lo que genera el riesgo de que la información se pierda o pueda ser alterada o destruida por los mismos ciberdelincuentes.

Bajo esta problemática, la medida procesal de búsqueda de piezas de convicción y restricción de derechos aplicable ante este tipo de delitos es el levantamiento del secretario bancario, regulado en el artículo 235 del Código Procesal Penal (2004); sin embargo, esta medida no es inmediata, ya que, al tratarse de documentación e información confidencial de los usuarios de servicios bancarios, con relación a los servicios que prestan las empresas del

sistema, estas no pueden facilitar la información referente a las operaciones bancarias a terceros, salvo por mandato judicial; lo que demanda tiempo por parte del juez para otorgar esta autorización y así obtener la documentación solicitada por el fiscal a cargo de la investigación del delito.

En tal sentido, en el presente trabajo la hipótesis que se plantea es que, ante las limitaciones que presenta el levantamiento del secreto bancario, es posible recurrir a la aplicación de otras medidas previstas en el mismo Código Procesal Penal del 2004, en particular la medida procesal de incautación de bienes.

Como se conoce, la medida de incautación es una medida limitativa de derechos aplicada en la primera etapa del proceso penal (investigación preliminar y preparatoria), que consiste en la intervención física, aprehensión o toma de posesión sobre bienes que se presumen, constituyen objeto, cuerpo, instrumentos, efectos o ganancias del delito en el marco de una intervención penal, susceptible de ser devuelta (Ministerio de Justicia y Derechos Humanos, 2018). Además, esta medida limitativa interviene sobre bienes que son objeto materia del delito, este concepto amplio puede incluir el producto directo del delito como las sucesivas modificaciones que este experimente en el tráfico jurídico al pasar el tiempo.

Estando a que los ilícitos de carácter informático son delitos especiales, la propuesta interpretativa aquí defendida es que no podría excluirse a los delitos informáticos la aplicación de la incautación, especialmente en el delito de *SIM swapping;* debido a que, al tratarse de un delito realizado mediante medios tecnológicos, los datos informáticos son volátiles; es decir, son alterados o modificados con facilidad. Por tanto, esta medida limitativa permitiría obtener los datos informáticos de una forma rápida para la investigación.

Para ello se requiere tener un alcance más amplio del concepto de “bien”; siendo así que los profesores Jorge y Francisco Avendaño (2017, p. 22) definen el término “bien” de la siguiente manera:

> Entidades materiales o inmateriales, tomadas en consideración por la ley en cuanto constituyen o pueden constituir objeto de relaciones jurídicas. Tienen valor económico y son susceptibles de ser apropiados, transferidos en el mercado y utilizados por las personas con la finalidad de satisfacer sus necesidades.

Asimismo, los citados autores clasifican los bienes como corporales e incorporables; consumibles y no consumibles; fungibles y no fungibles y bienes muebles e inmuebles, lo que nos lleva a calificar a los datos informáticos como bienes incorporales partiendo de la premisa expuesta por los citados autores.

En efecto, el dato informático es un concepto novedoso que no fue incluido en el tradicional concepto que maneja nuestra legislación y que ha sido incorporada por diferentes tratadistas; por ejemplo, para Arias de Rincón (2007), los datos informáticos son “segmentos de información numérica que circulan en la red, considerados como bienes muebles incorporales”. Por lo cual entendemos que la medida de incautación fue diseñada de espaldas a la posible inclusión de los datos informáticos como bienes pasibles de ser incautados. No obstante, como se puede apreciar, no existe obstáculo conceptual ni de los principios del proceso, que impidan que el dato informático pueda ser objeto de esta medida de búsqueda de pruebas.

Las ventajas que plantea aplicar la incautación como medida complementaria/alternativa al levantamiento del secreto bancario son las siguientes: búsqueda, retención, conservación y aseguramiento de los elementos que puedan servir como medios de prueba, impedimento a la obstaculización de la averiguación de la verdad y obtener las fuentes de prueba de forma inmediata que pueden servir como medios

probatorios en etapa de juicio. Este planteamiento, se ve reforzado con el principio de mismidad, el cual se caracteriza porque el elemento recogido es el mismo que se encontró en la escena, la interpretación de la evidencia refleja lo que realmente pasó y el estado del elemento se conserva en las mismas condiciones en las que se encontró en la escena; todo ello con la finalidad de resguardar la autenticidad de la evidencia para la investigación.

Por su parte, Hermosillo (2021) afirma que todo elemento probatorio debe ser puesto en cadena de custodia para su posterior análisis en base a procedimientos científicos para coadyuvar al esclarecimiento de los hechos. Bajo este concepto, la aplicación de la medida de incautación en el delito de *SIM swapping* conlleva que la prueba digital (datos y/o sistemas informáticos) pueda ser recogida mediante una cadena de custodia con el objetivo de brindar veracidad y confiabilidad de la información recolectada en el proceso penal. Para ello, debe establecerse los métodos correctos para la sustracción de la evidencia informática; es decir, que la prueba no pueda verse afectada por suplantaciones, alteraciones, modificaciones o en el peor de los casos su destrucción.

En tal sentido, a través de la presente investigación se analiza la posibilidad de aplicar la medida procesal de Incautación de Bienes, en el delito informático denominado *SIM swapping* a efecto de que puedan los investigadores obtener información de los datos del sistema bancario y telecomunicaciones de una manera eficaz.

1.5. Justificación del estudio

Conforme a la estadística de seguridad ciudadana (INEI, 2023), se señala que el incremento de los delitos informáticos a causa del avance tecnológico, se tiene registrada la alarmante cifra de 512 denuncias por la comisión de delitos informáticos entre los meses de octubre y diciembre del 2022, cifra mayor en 121 denuncias a comparación con el periodo del 2021 (incremento de un 30,9 %), siendo mérito de análisis en un ámbito penal las

medidas adoptadas para contrarrestar estas cifras generadas por la perpetración de los delitos informáticos.

Por consecuencia, el delito informático *SIM swapping* necesita una mayor atención, en la medida que los ciberdelincuentes actúan sigilosamente usando mecanismos capaces de borrar y destruir todo rastro de intrusión o la consumación del delito. Sin embargo, nuestra legislación en el ámbito penal no cuenta con herramientas idóneas para la oportuna indagación de dichos sucesos delictivos. Por lo que consideramos que se debe trabajar junto con expertos en seguridad cibernética para salvaguardar la información ante la cantidad de ciberdelincuentes que bordean la web, ya que su única intención es perjudicar a terceros y enriquecerse de manera ilícita.

Si bien es cierto, se están incorporando nuevas medidas de prevención en el ámbito administrativo (Resolución N.° 072-2022-CD/OSIPTEL), con el propósito de evitar la comisión del delito informático de *SIM swapping*; no obstante, actualmente no se ha podido concretar una reposición del derecho afectado al titular, en el extremo de que estas resultan tener un carácter netamente administrativo, resultando evidente las carencias aplicadas a la investigación del proceso penal.

Asimismo, es menester mencionar que la Resolución N.° 072-2022-CD/OSIPTEL solo se avoca a un ámbito administrativo, en referencia a la sanción aplicada a la empresa prestadora de servicio de telefonía móvil, por no adoptar las medidas de seguridad especificadas en la norma citada. Sin embargo, desde un punto de vista penal, esta no tiene mayor relevancia en cuanto al resarcimiento del derecho vulnerado de la víctima, más aún cuando en un proceso penal se ve entorpecido por la inaplicabilidad de medidas procesales que se ajusten a una investigación correcta en este tipo de delitos informáticos, que por su naturaleza del delito es más factible que la información sea alterada, modificada o eliminada

dejando sin efecto los actuados preliminares y por ende concluyendo con el archivo del proceso.

En consecuencia, la presente investigación propone la aplicación de la incautación de bienes como medida coercitiva para el delito informático *SIM swapping*, a fin de preservar la prueba informática ante la peligrosidad de estas organizaciones delictivas, y de esta manera evitar el enriquecimiento indebido de los agentes del delito, con los efectos y ganancias del mismo y otras actividades *SIM*ilares que están inmersas en esta era digital como lo es la información digital, las TIC, entre otros de *SIM*ilar naturaleza.

1.6. Diseño de la Investigación

Investigación bibliográfica.

1.7. Método Empleado

Por tratarse de una investigación sobre un problema de carácter estrictamente jurídico, la presente investigación utiliza el método dogmático.

Por otro lado, Ramos (2011) considera que el objetivo de la dogmática jurídica, es el estudio de las normas positivas, instituciones o conceptos jurídicos que provienen de distintas fuentes del derecho, como es el caso de la jurisprudencia, la costumbre, etc., las que a su vez son fuentes de investigación como sucede con la doctrina jurídica que utiliza técnicas y herramientas documentales, no empíricas.

Para Rodriguez (1999, quien cita a Villoro), la sistemática jurídica, llamada por los alemanes dogmática jurídica, es el conocimiento ordenado conforme al derecho positivo; y trata de explicar el sentido de una norma o varias en concordancia con las demás normas jurídicas al sistema al que pertenecen.

Por su parte, Witker (1986), en síntesis, explica que la dogmática jurídica en general se origina en el pensamiento que el derecho es considerado una ciencia o técnica formal y,

en consecuencia; como una variable independiente de la sociedad, dotada de autosuficiencia metodológica y técnica.

En tal sentido, la presente investigación está basada en la aplicabilidad de la medida procesal de la incautación de bienes en la investigación del delito informático *SIM swapping* desde el análisis de un enfoque dogmático de la referida institución procesal.

1.8. Descripción de las Técnicas de Recojo y Análisis de la Información

La investigación bibliográfica no es una investigación de corte empírico, sino que se basa en el análisis sistemático de fuentes; en este caso, del ordenamiento jurídico procesal penal, el cual se analiza mediante criterios interpretativos de base estrictamente jurídica, es decir, utilizando mecanismos interpretativos propios del derecho: método literal, histórico, sistemático, entre otros que resultan aplicables en el derecho penal y procesal penal.

Para el recojo de la información vamos a recurrir, en primer lugar, a bibliografía indexada o arbitrada; revistas científicas de carácter nacional e internacional. Sin embargo, dado que este criterio de discriminación de las fuentes podría reducir drásticamente nuestro ámbito de estudio, dejando fuera de análisis fuentes bibliográficas que resultan relevantes en nuestro entorno, se tendrá cuidado en recoger información sobre la base del prestigio académico de los autores (profesores universitarios, operadores de justicia, especialistas destacados) o la difusión de las obras (escritos que, pese a su antigüedad, son permanentemente citados en la bibliografía usual o en la jurisprudencia).

Asimismo, los medios a través de los cuales se obtendrá dicha información serán ficheros electrónicos, bases de datos (de acceso abierto o restringido, como, por ejemplo, las que pone a disposición de los estudiantes la Universidad Continental), bibliotecas (públicas o privadas), bibliotecas universitarias, etc.

El parámetro de búsqueda es la correlación de la fuente con el problema de investigación que estamos analizando (vínculo con el alcance de tema), esto es, no solo se

analizará la coherencia interna de cada texto analizado (logicidad, solidez de sus argumentos, evidencia de fuentes, entre otros), sino su relación con el tema que se propone investigar.

CAPÍTULO II

LIMITACIONES PROCESALES DEL LEVANTAMIENTO DEL SECRETO BANCARIO COMO MECANISMO DE LA INVESTIGACIÓN DEL DELITO INFORMÁTICO *SIM SWAPPING*

2.1. Los delitos informáticos en la Ley N.° 30171

La Ley N.° 30171, Ley de delitos informáticos, que modificó a la Ley 30096, busca garantizar una lucha eficaz contra la ciberdelincuencia, previniendo y sancionando los actos ilícitos que afectan a los sistemas y datos informáticos, además de proteger otros bienes jurídicos que son de trascendencia penal; dichas conductas, además tienen la peculiaridad de operar por medio de las tecnologías de la información o de la comunicación.

La ley en mención desarrolla las diferentes modalidades de delitos informáticos previstos en nuestra realidad social. La ciberdelincuencia es un mecanismo estratégico para delinquir, donde la mayoría de las personas son víctimas de diferentes tipos de delitos basados en el uso de la tecnología.

Por ello, antes de analizar la legislación específica, es necesario definir qué es un delito informático. Un sector doctrinal construye la definición de delito informático sobre la base del medio empleado para la comisión del ilícito: dispositivos usados en actividades informáticas como las computadoras o instrumentos afines (así Téllez, 1998; Acurio, 1989, esta última cita a su vez a Castillo y Ramallo).

Por su parte, Bramont-Arias (1997, p. 78), de manera general, señala que, para la consumación del delito informático, es necesario un sistema automático de datos, es decir, que se emplee un sistema tecnológico y/o datos.

Por lo que bajo esta conducta ilícita, muy frecuentemente, los ciberdelincuentes operan interfiriendo en los dispositivos de las personas lo que provoca una afectación económica. Es por ello que el Estado adoptó medidas legislativas para la regulación de estos

delitos, como la Ley N.° 30171, orientada a regular y sancionar toda conducta ilícita que afecta los datos y sistemas informáticos.

2.1.1. El fraude informático

Este delito se encuentra previsto en el artículo 8 de la Ley 30096, modificada a través de la Ley 30171, donde expresamente señala que el fraude informático tiene, como característica principal, el obtener un provecho ilícito para sí o para otro, perjudicando a un tercero, mediante:

> Diseño, introducción, alteración, borrado, supresión y clonación de datos informáticos; y/o cualquier interferencia o manipulación en el funcionamiento de un sistema informático.

Respecto a la pena, esta será no menor de 3 años ni mayor de 8 años y 60 a 120 días multa. Sin embargo, cuando se afecta el patrimonio del Estado o fines asistenciales o programas de apoyo, la pena es no menor de 5 ni mayor de 10 años y 80 a 140 días multa.

Para Pérez (2019), en el delito informático, el autor, mediante el uso de la tecnología, diseña, altera, borra, introduce o clona los sistemas y/o datos informáticos obteniendo un provecho para sí mismo o para otro, perjudicando a un tercero.

Por su parte, Hugo (2014), señala que la conducta delictiva de delito de fraude informático prevé una modalidad comisiva (activa). Asimismo, este autor afirma que esta modalidad delictiva está basada en el *animus lucrandi*, no obstante, el tipo penal previsto en el art. 8 de la Ley de Delitos Informáticos hace referencia a la obtención o procuración de un provecho ilícito en perjuicio de tercero, lo cual, a nuestro entender, no solo permite afirmar la existencia de esta modalidad delictiva ante daños de carácter patrimonial, sino de otro tipo de provechos ilícitamente obtenidos.

De esta manera se entiende al fraude informático como aquella acción antijurídica y culpable, en la que una persona, a través del uso de medios tecnológicos, busca manipular

los datos informáticos contenidos en un sistema informático, accediendo a la información reservada de la víctima, lo que provoca un perjuicio económico.

2.1.2. El delito del *SIM swapping* en la legislación peruana

El portal del Ministerio de Transporte y Comunicaciones (MTC, 2022) define explícitamente al *SIM swapping* como la suplantación de identidad para reemplazar el chip o tarjeta *SIM* y así acceder a las cuentas bancarias de los usuarios. Enfatiza también que esta es una nueva modalidad de fraude sumamente peligrosa, en la que el delincuente digital accede al número y operador telefónico de la víctima y solicita un duplicado de tarjeta *SIM* para activar el número en otro terminal (teléfono móvil). Al hacerlo, la víctima aprecia una aparente suspensión de su servicio de telefonía, mientras el delincuente, con la línea activa en otro terminal, accede a sus cuentas y procede a realizar el delito, lo que genera perjuicios evidentes en contra de la víctima.

Por ello, y dentro del análisis que implica la presente investigación, encontramos que, dentro de los múltiples delitos informáticos, específicamente en la tipología de fraude informático, se puede ubicar, a su vez, la modalidad delictiva del *SIM swapping* antes descrita, que es una forma de sustracción fraudulenta de la identidad cibernética y cuyo objetivo es tener acceso a los datos de las cuentas bancarias de los usuarios.

Para consumarse el delito de *SIM swapping* es fundamental obtener la doble verificación que muchos bancos utilizan para autorizar pagos y transferencias a sus clientes. Generalmente, un código de verificación es enviado, por medio de un SMS, al teléfono móvil del usuario para realizar estas transacciones, los aplicativos (*apps*) de los bancos disponen de claves de acceso cifrado de las comunicaciones y teclados virtuales, sin embargo, los ciberdelincuentes, por medio de técnicas de persuasión y manipulación, obtienen este dato informático.

Entonces, el delito de *SIM swapping* se ubica dentro de la descripción típica del fraude informático, previsto en el artículo 8 de la Ley 30096 modificada a través de la Ley 30171 (Ley de Delitos Informáticos). Dicha conducta castiga al que, obtiene un provecho ilícito, para sí, o para otro, actuando deliberada e ilegítimamente, mediante la clonación del módulo de identidad del suscriptor (*SIM*), imponiéndole una pena privativa de la libertad no menor de 3 ni mayor de 8 años y con 60 a 120 días multa. De este modo, se entiende que el delincuente, al realizar la clonación del *SIM,* busca obtener el acceso a diversas contraseñas que le permitan efectuar la autorización para realizar movimientos en las cuentas bancarias que se encuentran vinculadas al teléfono móvil.

A continuación, se analiza la estructura del tipo penal del fraude informático con especial referencia al *SIM swapping* basado en la teoría tripartita del delito.

a) Sujetos

Sujeto activo

Acurio (2017) define al sujeto activo como aquella persona que tiene una habilidad especial en el conocimiento de los sistemas informáticos colocándose en puntos estratégicos donde se halla información de carácter importante o reservada; o aquella persona que tiene conocimiento en el manejo de sistemas informáticos sin estar inmerso en un campo estratégico.

Sin embargo, Gutiérrez y Ruiz (2014, p. 289 citados por Villavicencio) difieren de la idea propuesta por Acurio, en la medida que consideran que "el autor del delito informático puede serlo cualquiera, no precisando que cumpla con determinados requisitos personales o conocimientos técnicos cualificados".

Este último punto de vista es el más acertado respecto al sujeto activo en el delito de *SIM swapping*, puesto que la comisión de dicho delito puede realizarla tanto una persona con conocimientos especializados, como una persona que posee únicamente conocimientos

empíricos en la materia. Consideramos que esta postura es la que mejor se acomoda a la descripción del sujeto activo prevista en el artículo 8° de la Ley de Delitos Informáticos.

Sujeto pasivo

En la literatura penal, la doctrina distingue al sujeto pasivo en dos formas; la primera, como el sujeto pasivo de la acción y la segunda como el sujeto pasivo del delito (véase Bramont-Arias, 1997).

En relación con el delito de *SIM swapping*, se entiende como sujeto pasivo de la acción a aquel que va a recibir (sobre quien recae) de forma directa la acción típica del sujeto activo; en ese sentido, en el *SIM swapping*, son sujetos pasivos de la acción las entidades prestadoras de servicios de telefonía móvil y las entidades financieras.

Por su parte, el sujeto pasivo del delito es el titular del bien jurídico protegido. En el caso del fraude informático, se trata de quien, en virtud del acto delictivo, padece un perjuicio. A su vez, para el caso del *SIM swapping*, los sujetos pasivos del delito serían los usuarios y/o particulares que contratan el servicio de telefonía móvil.

Bien jurídico protegido

Debido a los delitos informáticos, los profesores Gutiérrez, Mazuelos y Durand (citados por Villavicencio Terreros, 2014, p. 288) afirman que la protección jurídica que debe otorgarse en los delitos informáticos es el siguiente:

Se percibe en dos planos de manera conjunta y concatenada; en el primero se halla de manera general la información; es decir, la información almacenada, tratada y transmitida a través de los sistemas de tratamiento automatizado de datos, y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etcétera.

Asimismo, los citados autores señalan, con respecto al bien jurídico general que la información que está constituida por el contenido de las bases y/o bancos de datos o el

producto de los procesos informáticos automatizados. Además, destacan la importancia de la información en un sentido económico; ello hace que la información se incorpore como bien jurídico autónomo, de valor económico, merecedor de tutela.

El grupo de investigación, de la tesis en desarrollo, considera que la valoración de otros bienes jurídicos (p. ej. patrimonio, indemnidad sexual, intimidad u otros), en segundo plano, se debe a que los delitos informáticos fueron construidos por el legislador tomando como base la normativa ordinaria de las correspondientes infracciones previstas en la legislación penal (tipos penales comunes); es decir, para construir el fraude informático, el legislador tomó como base un ataque patrimonial común u ordinario, pero a través de medios comisivos específicos (p. ej. diseño, alteración, supresión, introducción, clonación de datos informáticos).

Así, puede verse al analizar el Capítulo V de la Ley de Delitos Informáticos (modificada por la Ley 30171), cuando sitúa al fraude informático (art. 8) como un "delito informático contra el patrimonio". Este parecer del legislador, como se ha visto previamente, es seguido por la doctrina mayoritaria en nuestro país. Sin embargo, se entiende que los delitos informáticos, aun cuando pueden concurrir a la protección de intereses patrimoniales u otros bienes jurídicos, tienen un bien jurídico común que es la información.

Lo planteado anteriormente advierte que la Ley de Delitos Informáticos no protege una serie de bienes jurídicos autónomamente considerados; sino que se trata de una ley que protege un haz de conductas que atentan de modo genérico contra un bien jurídico como: la seguridad de la información, como un bien jurídico supraindividual.

Asimismo, esta idea se ve reforzada con el análisis del surgimiento de los delitos informáticos, los cuales nacen de la evolución de una sociedad catalogada como la emergente "sociedad de la información", la cual hace referencia a la evolución de la sociedad como tal. En el sentido que para su desarrollo es base primordial la tecnología, siendo esta la gestora

de la creación, distribución y manipulación de la información; en las actividades sociales, económicas y culturales, en mérito de conclusión se expresa que la tecnología es el medio que facilita el acceso a la información y como consecuencia el dinamismo del desarrollo.

Por consiguiente, es motivo de conclusión, que como consecuencia del impacto generado por la "sociedad de la información" es necesaria la incorporación de la *información* como un bien jurídico de protección. En tal sentido, conforme a la regulación del delito de fraude informático en la Ley N.° 30096, modificada por la Ley N.° 30171, hace referencia expresamente a los datos y sistemas informáticos como aquellos que serán manipulados, clonados entre otras acciones, los mismos que están clasificados como parte de la información.

En suma, a partir de lo desarrollado, se tiene la posición sostenida por Magliona y López (citados por Santiago Acurio, 2017), quienes precisando que los delitos informáticos se caracterizan por ser complejos, ya que protegen *SIM*ultáneamente diversos intereses jurídicos, siendo que un bien jurídico está independientemente protegido por otro. Es decir, se trata de un delito pluriofensivo, entendiéndose por este último término a aquel que afecta a más de un bien jurídico. Aunque los autores no expresan de forma literal que existe una bien jurídico general y otro específico, se logra interpretar ello entre líneas, conforme al argumento que sostienen en referencia a la afectación de más de un bien jurídico vulnerado.

En tal sentido, basándose en el delito específico del *SIM swapping*, el bien jurídico protegido es la seguridad de la información; al tratarse del tipo penal citado en el art. 8 de la Ley N.° 30171, el cual establece que aquel que clona de forma deliberada e ilegítima los datos informáticos o sistema informático, comete el delito de fraude informático (*SIM swapping*), sin embargo, el referente (objeto de la acción) en este delito en específico es el dinero (patrimonio) del sujeto pasivo depositado en una cuenta bancaria (dato electrónico) y que es transferido electrónicamente a la cuenta del sujeto activo, se obtiene como

consecuencia un provecho económico, que por consiguiente desencadena una afectación económica en la víctima, ello en concordancia con lo citado por los autores Gutiérrez, Mazuelos y Durand.

c) Verbos rectores

Conforme a la Ley de Delitos Informáticos, Ley N.° 30096, modificada por la Ley 30171, en relación con el delito de fraude informático, la norma señala que la forma en la que opera el sujeto activo es deliberada o ilegítima, siendo que, al lograr ingresar al sistema informático, tiene acceso a dicha información para poder alterar, borrar, desaparecer y clonar el funcionamiento del sistema informático, obteniendo un beneficio propio o para otro, perjudicando a un tercero. En tal sentido, Villavicencio (2014) señala que los verbos rectores en concordancia con la Ley de Delitos Informáticos son los siguientes:

Tabla 1

Ley N. 30171 (2014) - Verbos rectores en el delito de SIM swapping.

Verbo rector	Significado	Bien jurídico
Diseñar	Proyecto o plan	Datos informáticos o cualquier interferencia
Introducir	Entrar a algo	
Alterar	Estropear, dañar, descomponer	
Borrar	Desvanecer, quitar, hacer que desaparezca algo	
Suprimir	Hacer cesar, hacer desaparecer	
Clonar	Producir clones	
Manipular	Operar con las manos o cualquier instrumento	Funcionamiento de un sistema informático

El delito de *SIM swapping* es una modalidad de fraude informático, pues la conducta consiste en clonar, ya que el sujeto activo duplica la tarjeta *SIM* del titular (sujeto pasivo), transfiriendo los datos al momento de recuperar la información, accediendo a diferentes contraseñas que estén sincronizadas con la línea telefónica para obtener beneficio (p. ej.

cuentas bancarias, como transfiriendo el dinero que se encuentran en estas tarjetas de crédito, que causa un perjuicio económico a la víctima).

d) Elemento subjetivo

Para los profesores Lux y Calderón (2020), comentando el art. 7, de la Ley N.° 21.459, identifican que el delito de fraude informático previsto en la legislación chilena tiene una característica peculiar, que es el ánimo lucrativo, ya que ante el actuar comisivo con la intención dolosa o comisiva se altera el sistema o dato informáticos, lo que provoca un perjuicio económico. Esta opinión se traslada al tipo penal materia de investigación, pues el delito de fraude informático previsto en la legislación nacional tiene alcances *SIM*ilares a los de su par chileno.

En esa misma línea, Gercke (2020, citado por Conapoc) afirma que en el delito de fraude informático el objetivo es la manipulación fraudulenta de los datos y sistemas informáticos, lo que genera un perjuicio de carácter patrimonial a un tercero.

En efecto, la Ley N.° 30171 señala que el delito de fraude informático tiene como fin obtener un provecho ilícito de forma ilegítima y deliberada, por lo que, si bien es cierto un provecho ilícito se expresa de manera general, en el caso del delito de *SIM swapping* el provecho ilícito se traduce a un provecho patrimonial, ya que el autor del delito accede a información explícitamente relacionada a contraseñas y cuentas bancarias, logrando manipularlas a favor de sí mismo u otro, a fin de obtener un beneficio económico, tal como se explicó en los párrafos precedentes.

e) Consumación

Para Rodriguez (2013), el delito informático es una acción antijurídica y culpable y, para que este delito se consume, debe afectarse una computadora.

Sin embargo, Villavicencio (2014) señala que la Ley de Delitos Informáticos (Ley N.° 30171) al especificar las formas en las que se puede realizar la acción penal se centraría

en un delito de resultado, ya que, tal como lo prevé la norma, no es suficiente el fraude para la consumación del delito, sino que este debe conllevar un perjuicio a una tercera persona, de tal forma que si no se cumple esta consecuencia estaríamos hablando de una tentativa, más no de una consumación.

En tal sentido, el *SIM swapping* es un delito de resultado, ya que, al ser un tipo de fraude informático, el cual se realiza mediante la obtención de los datos informáticos almacenados en el IMEI para posteriormente acceder a las cuentas bancarias de los bancos móvil, se consuma cuando el sujeto activo obtiene un beneficio económico que causa un perjuicio al sujeto pasivo.

2.1.3. Pronunciamientos jurisprudenciales respecto al delito de fraude informático

No existe un reconocimiento expreso de la denominación *SIM swapping* en los pronunciamientos jurisprudenciales que se han podido encontrar en nuestro ordenamiento. Adicionalmente, no se han encontrado casos judiciales de fraude informático bajo dicha modalidad que hayan merecido una condena penal.

No obstante, en los tribunales administrativos sí es posible ubicar casuística que haya merecido el análisis y pronunciamiento de dichos órganos. Así, puede mencionarse el Exp. N.° 0064-2020/CPC-Indecopi-CHT, seguido contra una entidad bancaria por presuntas infracciones de la Ley 29571, Código de Protección y Defensa del Consumidor.

En dicho expediente, la Sala Especializada en Protección al Consumidor del Tribunal de Defensa de la Competencia y de la Propiedad Intelectual emite la Resolución N.° 1477-2022/SPC-Indecopi, en la que resalta lo siguiente: el demandante (cliente de una entidad bancaria), al revisar su aplicativo móvil, identifica una transferencia interbancaria por el monto de S/. 3,808.95 soles a la cuenta de un tercero (el señor Antony MM). Al tratarse de una transacción no reconocida por el cliente, este se comunica por vía telefónica con el banco

para denunciar y bloquear la tarjeta. Sin embargo, en el transcurso de la llamada, el demandante, al actualizar su banca móvil, se percata de dos movimientos adicionales por S/. 265.80 soles y una disposición de efectivo por el monto de S/. 200.00 soles, a la misma cuenta del tercero (Antony M.M.). Ante tal hecho, personal de la entidad bancaria bloqueó la tarjeta y el acceso al banco móvil, lo que genera el reclamo mediante una llamada realizada desde el celular del progenitor del demandante, ya que su servicio móvil había perdido señal repentinamente.

Así, el usuario se apersonó a la empresa telefónica para saber el motivo de la pérdida de señal y de internet en su celular, siendo informado de que el titular de la línea (es decir, alguien que se había hecho pasar por el demandante), había realizado una reposición de chip, en fecha coincidente con la de la pérdida de señal en su línea telefónica. Al día siguiente el usuario se comunicó con su banco para consultar su estado de cuenta, siendo informado de que el monto total de las operaciones no reconocidas ascendía en total a S/ 10,166.80, ante lo cual se bloqueó definitivo de su tarjeta de crédito y se procedió a formular el reclamo respectivo.

Por otro lado, se apersonó a la empresa telefónica para el bloqueo de su celular, siendo informado de la existencia de dos equipos celulares (terminales) donde estuvo activo el referido número, siendo que uno de tales equipos no le pertenecía. A consecuencia de ello, la empresa de telefonía móvil le informa que su caso se debe a una falta de cumplimiento de sus derechos reconocidos en la normativa de servicios bancarios y que las sustracciones de dinero de su cuenta no son responsabilidad de la empresa de telecomunicaciones; descartando que la entrega del chip solicitado fraudulentamente (bajo la apariencia de una reposición por pérdida, en realidad, no solicitada por el cliente), le generara alguna responsabilidad en la sustracción del dinero. A consecuencia de estos hechos, el señor Rony Gianfranco BO solicita al banco X el congelamiento y/o reprogramación de la deuda

atribuida a él, como consecuencia de las operaciones bancarias fraudulentas hechas en su cuenta, no recibiendo respuesta de la entidad bancaria.

Sobre la base de lo anterior, el agraviado solicita al tribunal de Indecopi la imposición de una medida correctiva al banco para que le reembolse el importe sustraído de su tarjeta por las operaciones no reconocidas más los intereses generados y se sancione al banco por no brindar seguridad a los datos personales al cliente.

Ante estos hechos, mediante la Resolución 0164-2021/Indecopi-CHT del 10 de setiembre de 2021, la Comisión de la Oficina Regional del Indecopi de Áncash-Sede Chimbote declara fundada la denuncia, por infracción del artículo 19° de la Ley N.° 29571, Código de Protección y Defensa del Consumidor, debido a que la entidad financiera no adoptó las medidas de seguridad necesarias para impedir que se efectúen retiros no reconocidos (operaciones no reconocidas) con cargo a la tarjeta de débito y a la tarjeta de crédito del agraviado, por lo que le sanciona con 10 UIT (5 UIT por cada tarjeta); ordenando al banco, como medida correctiva reparadora, que en un plazo no mayor de quince (15) días hábiles, devuelva diversos importes no reconocidos (operaciones no reconocidas) con cargo a la tarjeta de débito y de crédito del denunciante.

Esta decisión fue materia de apelación, pronunciándose el Colegiado superior básicamente en el mismo sentido que el órgano sancionador de primera instancia, no obstante, revocaron ese extremo de la sanción impuesta y reformándola, por lo que sancionaron a la institución financiera con la multa de 2 UIT.

En esa misma línea casuística, tenemos el Exp. 0530-2021/CC1 Indecopi-CHT, seguido contra otra entidad bancaria, por presuntas infracciones de los artículos 18º y 19º de la Ley 29571, Código de Protección y Defensa del Consumidor. En dicho expediente, la Sala Especializada en Protección al Consumidor del Tribunal de Defensa de la Competencia y de la Propiedad Intelectual emite la Resolución N.° 1208-2022/SPC-Indecopi, resaltando de

igual manera que la entidad bancaria no adoptó las medidas de seguridad necesarias, ante la detección de una operación ajena al patrón de consumo de la tarjeta habiente acaecida del denunciante Ernesto Javier de O. M.

Bajo esta casuística, es importante analizar que, ante los hechos de fraude informático, tal como lo menciona Indecopi, la entidad bancaria tiene como deber implementar y mantener lineamientos de seguridad para resguardar las operaciones realizadas por sus usuarios; sin embargo, tal como se señaló, en el presente caso, si bien se encuentra responsabilidad por parte de la entidad bancaria por no adoptar las medidas de seguridad dispuestas por el Reglamento de Tarjetas de Crédito y Débito, esto no guarda relación con la necesidad de identificar, denunciar y sancionar al responsable de este fraude informático como delito. Así, en la práctica, en estos casos solo se puede advertir una eventual infracción administrativa hacia la entidad bancaria, más no es suficiente para atribuirle su intervención (como persona jurídica) en un delito. Por lo que, esta figura administrativa no es suficiente para satisfacer la ilicitud que se genera en el delito de *SIM swapping*, donde se ve vulnerado el derecho a la información, a través de actos ilícitos como lo es el fraude informático, distinguiéndose ampliamente que en un ámbito administrativo (sancionador) a través de Indecopi su finalidad es proteger al consumidor, mas no proteger bienes jurídicos de carácter penal.

Si se traslada lo anterior al plano de la investigación penal, como parte de una estrategia para combatir la ciberdelincuencia, resulta evidente que, en este tipo de delito de fraude informático (*SIM swapping)*, al ser un delito relativamente novedoso en nuestra legislación, necesitamos aplicar las medidas procesales con el fin de recabar los medios probatorios idóneos para el esclarecimiento del hecho ilícito, ya que estamos frente a un delito donde prima la manipulación de medios tecnológicos dificultando que se pueda

obtener elementos que contribuyan a la investigación para sancionar al responsable de este ilícito.

2.1.4. Legislación comparada

La proliferación de los ciberdelitos en sus diversas modalidades ha significado un peligro constante para la seguridad y privacidad de los ciudadanos alrededor del continente; este mal que aqueja a más de una nación ha impulsado la adopción de diferentes medidas legislativas a fin de dar una oportuna solución a tan acelerado y exitoso movimiento ilícito que se viene trabajando desde el extremo de la ingeniería social.

Por ello y en observación de la actuación de los países que guardan cierta *SIM*ilitud con la realidad social del nuestro, la presente investigación ha dirigido su punto de comparación con cuatro países latinos y uno europeo en la medida que este último resulta ser principal influyente en nuestro sistema jurídico (romano germánico).

Delitos informáticos en Argentina

Es oportuno enfatizar la labor de persecución que vienen desarrollando los operadores de justicia de la República de Argentina, quienes han sabido dirigir y aplicar su normatividad en pro de su nación.

Argentina no contempla en su ordenamiento jurídico una regulación especial como tal, sin embargo, el legislador del país sureño, a través de la Ley N.° 26.388 (2008), introduce una serie de delitos informáticos a la legislación penal vigente; tales como los delitos que vulneran el acceso informático, delitos de fraude y daño informáticos, entre otros.

Seguidamente, es apreciable la inserción que la ley hace al epígrafe del Cap. III, en el que se incorpora el título de “Violación de Secretos y de la Privacidad”, correspondiendo al desarrollo del tipo penal de *SIM swapping.* En el artículo 173 se hace mención acerca del fraude que se cometiese a través de cualquier técnica de manipulación informática, alterando de este modo el normal desempeño de un sistema informático o transmisión de datos.

Con respecto a los delitos contra el acceso informático, el mismo cuerpo legal expresa de manera literal, la sanción ejercida en contra de aquel individuo que valiéndose de determinados mecanismos acceda ilícitamente a un sistema informático privado, asimismo se tiene como agravante si el perjuicio es frente a un organismo público, ya que este último representa al estado como institución y su vulnerabilidad compromete un mayor daño.

En los delitos contra el acceso a bancos de datos, la norma argentina lo desarrolla en su artículo 157, exponiendo la sanción para aquella persona natural que acceda a un sistema de datos de forma ilícita, que facilite o expone información restringida de un archivo o que también inserte o haga insertar datos a un archivo de datos personales; adicionalmente la norma da un tratamiento especial al autor del delito; pues si se trata de un funcionario público, este se sujeta a una sanción especial, que es la inhabilitación, situación *SIM*ilar que aplica el Perú con el término de agravantes con la diferencia que nuestra norma se extiende no solo a funcionarios público sino más bien a toda aquella persona que en ejercicio de sus funciones o abusando de sus atribuciones comete alguno de los ilícitos mencionados anteriormente.

En esa misma línea, el delito de daño informático, estipulado en su artículo 183, sanciona conductas como alterar o destruir sistemas informáticos como también sanciona a aquellas personas que comercializan o introduzcan programas destinados a dañar un sistema informático. Como se aprecia, los legisladores argentinos optaron por introducir esta nueva modalidad de delitos a su Código Penal vigente, a diferencia de la legislación peruana que opta por incluirlos en una ley penal especial, que da tratamiento específico a estos tipos penales.

Delitos informáticos en Colombia

En lo que compete al país colombiano, se tiene la publicación de una ley que modifica el Código Penal, dando origen al bien jurídico denominado la “protección de la información

y de los datos", a fin de resguardar los sistemas que utilizan las TIC´s de manera íntegra, visión que algunos doctrinarios rescatan y defienden; bajo el argumento que es necesario identificar a la "información" como un bien jurídico que buscará preservar integralmente a los sistemas que empleen las TIC..

La Ley N.° 1273 (2009) integra la tipificación de nuevos delitos informáticos frente a los diferentes sucesos presenciados en esta nueva era tecnológica.

Con el marco normativo presentado por el país colombiano, concluimos que esta ley implica una gran contribución a su ordenamiento jurídico, adoptando las medidas legislativas necesarias a su realidad social para enfrentar este tipo de ilícitos, en lo referido al *SIM swapping*; de la interpretación de la norma, se extrae que este estaría inmerso en el delito calificado como hurto a través de medios informáticos y semejantes.

Delitos informáticos en Venezuela

Mediante la "Ley Especial contra los Delitos Informáticos", se da tratamiento a aquellos ilícitos cometidos a través de las tecnologías de la información y demás medios informáticos relacionados, la mencionada norma comprende veintiún tipos penales, dividiéndose en cinco categorías protegiendo un bien jurídico en específico, dándose el caso de la regulación de los delitos que van contra los sistemas que utilizan tecnologías de Información, aquellos que van contra la propiedad, los que vulneran la privacidad de las personas y de las comunicaciones, delitos que van contra niños (as) o adolescentes y finalmente la norma menciona a aquellos delitos que van en contra del orden económico.

Tratándose en la presente investigación; respecto al tipo penal de fraude informático, la legislación venezolana desarrolla en el Capítulo II de manera explícita los delitos de fraude, hurto, obtención indebida tanto de servicios y bienes, así mismo hace referencia al manejo de forma fraudulenta de tarjetas inteligentes, a la apropiación de estas, la posesión de equipos que faciliten las falsificaciones.

Al contrastar la información apreciamos que nuestra legislación al igual que la legislación venezolana, tenemos como común denominador que los delitos más relevantes son el delito de acceso indebido (que para nuestra legislación se denomina “acceso ilícito”), sabotaje o daño a sistemas (que para nuestra legislación se denomina “atentado a la integridad de sistemas informáticos”), posesión de equipos o prestación de servicios de sabotaje (no regulado por nuestra legislación) y el espionaje informático (no regulado por nuestra legislación). De igual manera, el fraude informático encabeza la preocupante lista de ciberdelitos en la nación venezolana y al igual que nuestro país diversos medios de prensa escrita, manifiestan el preocupante éxito en la comisión de dichos delitos, sobre todo en el delito informático del *SIM swapping*, ya que en este tipo penal en especial se volatilizan los datos, existiendo de tal modo el latente peligro en la detección del autor intelectual.

Delitos informáticos en España

En lo que respecta a la legislación española, se ha de precisar que la misma carece de una ley especial, sin embargo, la regulación que rige en torno a la lucha contra la comisión de dichos delitos es diversa, ya que se puede identificar normas indistintas que guardan relación con el tema, como las siguientes: Ley de Servicios de la Sociedad de la Información, Ley Orgánica de Protección de Datos de Carácter Personal, Reglamento de medidas de seguridad de los ficheros automatizados que incluyan datos de carácter personal, Ley General de Telecomunicaciones, Ley de Propiedad Intelectual, entre otras.

El Código Español tipifica diversas conductas delictivas relacionadas a los delitos informáticos, por ejemplo, delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

Con respecto al tema abordado, la legislación española prevé en su Código Penal conforme a su artículo 197, el delito de estafa electrónica que se realiza mediante la manipulación informática, como se pudo apreciar con anterioridad a este punto, los

legisladores y el cuerpo policial de España vienen trabajando fuertemente no solo en la prevención sino también en la persecución de los delitos informáticos y dado que el *SIM swapping* es un delito en el que la prueba es escurridiza y volátil, España ha desplegado distintas estrategias que han logrado optimizar, de tal manera que los resultados han sido verdaderamente satisfactorios, dentro de sus principales estrategias podríamos decir que la constante especialización y capacitación de sus agentes y operadores de justicia, les permite tener una visión más focalizada al ilícito materia de investigación, otra de sus grandes estrategias es el trabajo conjunto que promueve España, que busca relacionarse con otros, a fin de poder desplegar un plan de contingencia para contrarrestar este tipo de delitos.

Delitos informáticos en Chile

Al igual que nuestra legislación, el país vecino posee una ley específica para sancionar los delitos informáticos, a través de su Ley 21.459 del 2020, la norma chilena busca prevenir y sancionar los ilícitos, cuenta con ocho artículos que desarrollan los siguientes tipos penales: a) ataque a la integridad de un sistema informático, b) acceso ilícito, c) interceptación ilícita, d) ataque a la integridad de los datos informáticos, e) falsificación informática, f) receptación de datos informáticos, g) fraude informático, h) abuso de los dispositivos. Por otro lado, es preciso resaltar la labor del legislador chileno al prever el desarrollo del procedimiento adoptado por los órganos competentes a resolver los procesos que emergieron de los tipos penales expuestos, procedimiento ubicado en el Título II de la ley en mención.

Por lo expuesto en líneas anteriores, concluimos que la normativa chilena cumple con los paradigmas planteados en razón a dichos tipos penales, habiendo pasado por la modificación de su anterior ley que carecía de consistencia en el desarrollo de los tipo penales, pasando a una ley con mayores alcances en cuanto a los términos informáticos empleados y tomando en cuenta las modalidades delictivas que se vienen realizando en su

territorio para dar un tratamiento jurídico preciso, sin embargo ello no lo exime de poseer carencia como es el caso del tratamiento legal en torno a la suplantación de identidad a través de medios tecnológicos e informáticos.

2.2. El levantamiento del secreto bancario aplicado al delito informático *SIM swapping*

En palabras del suboficial Alexander Arturo Zambrano Gómez de la Divindat sede Arequipa, dentro del procedimiento adoptado por el equipo de dicha unidad, el levantamiento del secreto bancario significa la principal diligencia para obtener datos que permita conocer la identidad del presunto delincuente, dado que dicho documento alberga no solo los movimientos efectuados en la cuenta bancaria sino también se logra la visualización del IMEI (código exclusivo que identifica cada equipo móvil y es único), el cual se identifica cuando se efectúan operaciones bancarias a través de la banca móvil, banca por internet y demás *SIM*ilares; todo ello en el proceso que siguen los delincuentes al suplantar la tarjeta *SIM*, quedando este registro en los movimientos de la cuenta bancaria afectada (A. Zambrano, comunicación personal, 2022).

Frente a la problemática expuesta respecto de esta modalidad de fraude informático, se evidencia que la principal limitante para investigar este tipo de delito es el procedimiento en sede judicial, dado que la inmediatez en la respuesta es deficiente; motivo por el cual, los casos en investigación presentan demoras en su tramitación o no se logran concluir.

De ello se aprecia que la legislación pertinente para luchar contra la cibercriminalidad no ha rendido los resultados esperados, dado que el proceder de la Divindat (División de Investigación de Delitos de Alta Tecnología), encuentra limitaciones para concluir los casos presentados en sede policial, puesto que la regulación del levantamiento del secreto bancario requiere necesariamente la orden de un juez, y es allí

donde la investigación se demora o detiene, sin perjuicio de la demora que se produce en sede judicial.

El presente trabajo de investigación busca explorar nuevas interpretaciones acerca del uso de las medidas procesales vigentes en el ordenamiento, que contribuyan a la persecución eficaz del fraude informático, aunado a la preservación de la prueba y su oportuna valoración.

2.2.1. Tratamiento del levantamiento del secreto bancario en el ordenamiento jurídico peruano

La Constitución Política del Perú, en el art. 2, inciso 5, contempla la medida del Levantamiento del Secreto Bancario y Reserva Tributaria; sin embargo, conforme a la Ley N.° 31507 (Ley de Reforma Constitucional que Fortalece la lucha Anticorrupción en el Marco del Levantamiento del Secreto Bancario y la Reserva Tributaria), se específica que tiene como énfasis la modificatoria del artículo citado respecto a los sujetos que pueden efectuar el pedido del secreto bancario y la reserva tributaria, los cuales pueden ser los siguientes: el juez, el fiscal de la nación, una comisión investigadora del Congreso con arreglo a ley, el contralor general de la república respecto de funcionarios y servidores públicos y el superintendente de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones para los fines específicos de la inteligencia financiera. En aplicación del artículo citado, será el fiscal penal, el sujeto idóneo para efectuar el pedido del levantamiento del secreto bancario en el delito de *SIM swapping*.

Asimismo, el fiscal, como titular de la acción penal, puede aplicar diferentes medidas para la prevención, detección y persecución del delito. En el caso del fraude informático, surge la necesidad de que las autoridades instructoras tengan acceso a la información bancaria relacionada con la comisión del delito, siendo el levantamiento del secreto bancario

la medida procesal que el Código Procesal Penal del 2004 estandariza para el esclarecimiento de la investigación en este tipo de delitos.

En efecto, el levantamiento del secreto bancario se considera el recurso idóneo en estos casos, debido al tipo de información que se logra obtener a través de él: los movimientos bancarios que fueron efectuados sin consentimiento del agraviado, así como, eventualmente, los titulares de las cuentas de destino, en caso hayan sido utilizadas.

a) Regulación normativa

El levantamiento del secreto bancario se encuentra regulado en el artículo 235 del Código Procesal Penal, el cual delimita que la aplicación de dicha medida exclusivamente a las indagaciones que sean imprescindible para el esclarecimiento de un delito.

Por su parte, San Martin (2020) afirma que esta medida procesal es un acto de investigación limitativo de derechos, que se encuentra a cargo del fiscal; el mismo que, bajo autorización jurisdiccional, puede, de forma reservada y sin trámite previo, realizar el levantamiento del secreto bancario con el objetivo de esclarecer los hechos materia de investigación. No obstante, Vergara (1990) indica que, para que se aplique la medida procesal del levantamiento del secreto bancario, deben verificarse tres puntos:

i. Encontrarse sujeto a un proceso donde sea determinante la decisión de un juez.
ii. El juez debe avocarse a las operaciones específicas en relación con los antecedentes bancarios que estén inmersos en juicio.
iii. Deben estar relacionadas a operaciones y depósitos de cualquier naturaleza que haya realizado la parte procesal ya sea el acusado o el agraviado.

Es así, que la medida de levantamiento del secreto bancario proporciona importante información que se traduce en elementos de convicción dentro de la investigación fiscal y, a la postre, en elementos probatorios, que permiten acreditar el delito (condena).

En el enfoque del delito de *SIM swapping*, a través del levantamiento del secreto bancario se logra identificar el International Mobile Equipment Identity o IMEI, por sus siglas en inglés; que, traducido al español, significa algo *SIM*ilar a "identidad internacional de equipo móvil". Se trata de un código exclusivo que permite individualizar al aparato que fue utilizado como medio para cometer el delito, descartando o confirmando si el delito fue cometido desde un específico terminal (equipo), donde se realizaron las transacciones en las cuentas de la víctima, pues los reportes bancarios de las transacciones dubitadas informan al investigador desde qué terminal se realizaron las mismas.

b) Aplicación jurisprudencial

Dentro del desarrollo jurisprudencial, se tiene la Resolución N.° 32, del 8 de julio del 2019, emitida por la Primera Sala Penal de Apelaciones Nacional Permanente Especializada en Crimen Organizado, en el Exp. 00228-2016-1-5001-JR-PE-04, en la que se destaca lo siguiente:

El Fundamento 3.4.1.4. analiza el art. 330 inciso 2 del Código Procesal Penal y señala que la finalidad inmediata de las diligencias preliminares es realizar los actos urgentes e inaplazables a fin de determinar si han tenido lugar los hechos y asegurar los elementos materia de investigación. Es así que en esta etapa de investigación se convierte en un espacio legítimo para que el fiscal busque y adquiera elementos de convicción, siendo uno de ellos la limitación de derechos relativos.

El fundamento 3.4.1.6. expresa que hay dos presupuestos para la aplicación de estas medidas:

- Intervención indiciaria. El requerimiento fiscal debe precisar de manera motivada los elementos de convicción, indicando por qué debe adoptarse favorablemente la decisión judicial.

- Principio de proporcionalidad. Debe reunir lo siguiente: previsión normativa-jurisdiccionalidad y necesidad de motivación cualificada.
- Sujeción al test de proporcionalidad. Idoneidad, necesidad y proporcionalidad en sentido estricto.

Finalmente, el fundamento 3.4.2.4 de la referida resolución desglosa el artículo 235 del Código Procesal Penal que establece que el juez de la Investigación Preparatoria, a solicitud del fiscal, puede ordenar reservadamente y sin trámite alguno, el levantamiento del secreto bancario.

2.2.2. Limitaciones en el alcance de la medida de levantamiento del secreto bancario para responder adecuadamente a la criminalidad informática

En la actualidad, es preocupante la facilidad con la que los delincuentes informáticos acceden y manipulan los datos de las personas de manera indiscriminada. Según los datos aportados por la Divindat, en el periodo entre octubre de 2013 y diciembre de 2020 se registraron 12169 delitos vinculados a la Ley 30096, siendo el 78% (9515) delitos registrados por fraude informático (Conapoc, 2020, p. 37).

Cabe destacar que el acceso de estos datos de carácter personal y confidencial, asociados a una determinada persona, representan hoy en día información altamente vulnerable. Se trata de datos sobre los que el titular tiene el derecho soberano y exclusivo de controlar y decidir su uso o lo que el Tribunal Constitucional ha denominado derecho a la autodeterminación informativa (Exp. 04739-2007-PHD/TC, fundamento 2 y 3). En efecto, el Alto Tribunal señala que las entidades bancarias y las empresas que brindan servicios de telefonía móvil no han logrado garantizar la protección que este derecho requiere, exponiendo la seguridad de la información de sus clientes y/o usuarios.

En el caso del delito del *SIM swapping*, la sustracción de la información confidencial de una persona, a través de un sistema informático, puede devenir imposible de detectar si no se obtiene de manera inmediata los datos de las herramientas informáticas que se utilizan para dicha sustracción, debido a que todo en la nube es volátil; sin embargo, si dicha información es reunida dentro de un plazo inmediato (mediante los instrumentos procesales adecuados, en el seno de una investigación penal), pueden permitir obtener un perfil completo sobre una o varias características del responsable (el autor y/o sus cómplices), y de esta manera garantizar que el hecho materia de investigación no quede impune.

En ese sentido, se considera que la accesibilidad al secreto bancario autorizado por el órgano jurisdiccional de manera inmediata, fortalecería los mecanismos de investigación, convirtiéndose en una herramienta eficiente que permita detectar de manera oportuna casos de delitos informáticos como es el *SIM swapping*, puesto que, pese a las grandes virtudes que presenta dicha medida procesal, presenta carencias, como la ausencia de regulación de la intervención de los bancos para colaborar con la policía o la fiscalía, facilitándoles la información pertinente de una manera rápida y oportuna.

En efecto, una de las limitaciones para la aplicación del levantamiento del secreto bancario es la falta de celeridad con que se procede para su tramitación. En efecto, se puede explicar el trámite de manera resumida de la siguiente manera:

i) Una vez que la policía toma conocimiento del hecho, elabora un informe policial, el cual es remitido al fiscal para que solicite la medida procesal (levantamiento del secreto bancario) al juez;

ii) El fiscal analiza el informe policial y las razones por las cuales debe solicitar la técnica de investigación de levantamiento del secreto bancario. De encontrar razones justificadas, presenta dicho requerimiento al juez (según el protocolo interinstitucional, el

plazo es de 24 horas, no obstante, la carga procesal usual de las dependencias fiscales obliga a que estos plazos se vean sobrepasados).

iii) El juez al tomar conocimiento del requerimiento fiscal, lo evalúa, analizando que esté debidamente sustentado, dicho trámite es reservado.

iv) En caso de que el juez encuentre razonable el pedido, debe emitir inmediatamente un auto con motivación reforzada (por tratarse de una medida que afecta derechos fundamentales), el cual será notificado al fiscal que solicitó la medida (según el protocolo interinstitucional, el término para que el juez se pronuncie es de 24 horas, no obstante, la carga procesal usual de las dependencias judiciales obliga a que estos plazos se vean sobrepasados).

v) La ejecución de la medida está a cargo del fiscal, quien debe oficiar a la Superintendencia de Banca y Seguros (SBS) a fin de que, por intermedio de esta entidad se le proporcione la información requerida.

Según el Protocolo de Actuación Conjunta (2014), en caso de que exista demora por parte de las entidades bancarias para remitir la información requerida, el fiscal puede constituirse a sus sedes, para que cumplan con lo solicitado.

Aquí se evidencia claramente el problema que da lugar a formular la presente investigación, pues el Sistema Financiero hace depender la eficacia de las labores de investigación del fiscal del tiempo que le toma recabar la información de las entidades del sistema financiero, siguiendo, además, sus respectivos procedimientos internos; consecuentemente, al no tener el fiscal penal el control sobre la obtención rápida de los datos que requiere para identificar a los ciberdelincuentes y los movimientos que se aprueban sin el consentimiento del perjudicado, los casos se ven frecuentemente afectados por la imposibilidad de detectar a los responsables.

Como es de verse, los criterios establecidos en nuestro ordenamiento jurídico para la aplicación del levantamiento del secretario bancario no resultan eficaces para coadyuvar al esclarecimiento del delito, lo que genera de este modo vacíos en la norma que contribuyen a una deficiente interpretación y aplicación de la misma, asimismo como se expuso arriba, no existe un plazo determinado para que la entidad bancaria remita la información solicitada, dando como resultado la ineficiente actuación de la fiscalía al no resolver de manera oportuna estos hechos materia de investigación o, en el peor de los casos, al no aplicar esta medida, se brinda la facilidad al autor del hecho ilícito para que altere o elimine las huellas del delito, que causa absoluta impunidad a estos graves hechos.

2.2.3. Legislación comparada

Argentina

La Ley Nro. 21526, Ley de Entidades Financieras, regula el secreto bancario conforme a lo señalado en los artículos 39 y 40. Al respecto señala que las entidades financieras están limitadas a revelar aquellas operaciones pasivas de sus clientes, con excepción de aquellas causas judiciales donde medie un pronunciamiento judicial, al Banco Central de la República Argentina dentro de sus facultades y a los organismos recaudadores de impuestos nacionales, provinciales o municipales. Como se puede apreciar, el secreto bancario en Argentina esta tipificada en la ley descrita en el presente párrafo la cual afirma que dicha institución procesal protege a los clientes que realizan operaciones pasivas; de igual manera, establece de manera fehaciente los casos de excepción.

Por otro lado, es importante señalar que conforme a la legislación argentina se advierte que las operaciones realizadas en los bancos solo podrán ser reveladas por jueces en causas judiciales, encontrando *SIM*ilitud con nuestra legislación nacional en la que refiere que el secreto bancario solo podrá levantarse el secreto bancario por mandato judicial siempre que tenga relevancia con el caso investigado.

Colombia

En la legislación del país citado, se tiene el Código de Procedimientos Penales (Ley N.° 906-2004), el cual establece las facultades de la Fiscalía General de la Nación, dentro de sus facultades se encuentran las siguientes: ordenar registros, allanamientos, interceptaciones de comunicaciones con el objetivo de poner aquellos elementos que se hayan recogido a disposición del juez de control de garantías. En esa misma norma en su art. 154, se tiene que previamente se realizará un control de los elementos recabados por la Fiscalía para que se pueda llevar a cabo la audiencia de control de garantías por el Juez, la misma que es de carácter reservado.

Venezuela

En la Constitución Política de la República Bolivariana de Venezuela (1999), en el art. 48 protege el derecho al secreto y la inviolabilidad de las comunicaciones privadas en todas sus modalidades, salvo aquellas situaciones donde exista mandato emitida por el tribunal competente salvaguardando el secreto privado e información sin relevancia procesal.

Chile

En esta legislación, conforme a su Constitución Política (1980) al art. 19, inciso 4 y 5, que manifiesta que garantiza la protección de la inviolabilidad de toda comunicación privada, salvo aquellos determinados por ley. Sin embargo, la legislación chilena regula las medidas intrusivas destacándose el levantamiento del secreto bancario, cuyo objetivo es el desarrollo de investigación con el fin de aportar pruebas que se encuentren halladas en la privacidad de las personas, las cuales se encuentran protegidas legalmente.

Cavada (2018) afirma que estas técnicas de investigación si bien es cierto vulneran garantías personales como el derecho a la propiedad, la inviolabilidad de las comunicaciones, etc., su aplicación se justificaría desde una perspectiva política criminal al

estar inmersos en un ilícito investigado los cuales deberán ser resueltos para recolectar elementos típicos.

España

En la legislación española, uno de los preceptos actuales es la Ley Nro. 10/2014, conforme al art. 83, manifiesta que las entidades bancarias tienen el deber a reservar la información relacionada a saldos, transacciones y demás operaciones sin que las mismas no puedan ser materia de divulgación a terceros.

Este deber de reserva de información tiene excepciones, cuando el titular o la norma permita la divulgación a terceros o que, en su caso, les sean requeridas o hayan de remitir a las respectivas autoridades de supervisión o en el marco del cumplimiento de las obligaciones establecidas en la Ley de Prevención del Blanqueo de Capitales y la Financiación del Terrorismo.

Por otro lado, conforme a la Ley de Enjuiciamiento Criminal (1882), en su artículo 773, se señala que el Ministerio Fiscal de forma especial impulsa y desarrolla el trámite, así como otorgar a la Policía Judicial instrucciones, las cuales tienen que desarrollar eficazmente las mismas que deben guardar concordancia con el cumplimiento de sus funciones, dentro de esas funciones se encuentra el instar la aplicación de medidas cautelares tan pronto sean posibles a efecto de resolver la investigación.

2.2.4. Aplicabilidad de otras medidas de búsqueda de pruebas y restricción de derechos para responder a la criminalidad informática

Como se evidencia en el presente capítulo, el levantamiento del secreto bancario es la medida procesal exclusiva que se puede adoptar en nuestro ordenamiento para la persecución del tipo penal desarrollado. Mediante aquel se logra identificar los movimientos bancarios efectuados sin el consentimiento del agraviado, así como, eventualmente, la titularidad de las cuentas de destino, en caso se utilicen. Pero, debido a las limitaciones de

la medida procesal del levantamiento del secreto bancario (arriba anotadas), se puede apreciar un alto grado de ineficacia en la persecución de este tipo de criminalidad.

Por ende, resulta pertinente analizar si es posible la aplicación de otras medidas de búsqueda de pruebas y restricción de derechos, para viabilizar el éxito de las investigaciones de estos delitos. Así, conforme a la hipótesis que da lugar a la presente investigación, en los siguientes capítulos se analiza la posibilidad de aplicación de la medida de incautación de bienes en la investigación del delito de *SIM swapping*.

Montesquieu (1906, p. 237), afirma lo siguiente: "Los jueces de la nación no son, según sabemos, sino la boca por donde habla la ley, seres inanimados que no pueden moderar ni su fuerza ni su rigor". Bajo este argumento no se pretende que la interpretación analógica se limite al artículo VII del Código Procesal Penal: vigencia de la interpretación de la ley procesal. "La interpretación extensiva y la analogía quedan prohibidas mientras no favorezcan la libertad del imputado o el ejercicio de sus derechos"; por el contrario, se busca que ante la aplicación de la medida de incautación esta coadyuve al esclarecimiento de los hechos, sin restringir los derechos del imputado.

Partiendo de la premisa señalada por Montesquieu, esta investigación defiende la capacidad que, como conocedores del derecho, legisladores y demás sujetos impartidores de justicia integren todas las fuentes, principios y fundamentos del derecho para concretar un verdadero debido proceso que garantice un juzgamiento correctamente motivado.

En merito a lo señalado precedentemente, se pretende conocer que sí es posible la aplicación de la medida procesal de la incautación para la investigación de este tipo penal, a fin de acceder a las fuentes de prueba que permitan esclarecer el delito e identificar a los autores y partícipes del mismo, bajo una interpretación analógica; teniéndose en cuenta, que la medida de incautación tiene fundamento legal y es por ello que resulta válida esta interpretación, cabe precisar, que en este supuesto no se limita los derechos del imputado y

no se afecta las garantías del proceso penal; ya que su finalidad de esta medida procesal, es coadyuvar al esclarecimiento del hecho y preservar la prueba en una esfera digital.

CAPÍTULO III

MARCO CONSTITUCIONAL Y SUPRANACIONAL PARA ADOPTAR MEDIDAS EFECTIVAS FRENTE A LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS

3.1 Regulación Constitucional

3.1.1. Derechos protegidos constitucionalmente ante la comisión de un delito informático

Estos derechos inherentes a la persona, que nos protege ante un hecho delictivo se encuentran reconocidos en nuestra Carta Magna, y son por su naturaleza los más importantes dentro de la sociedad.

Los derechos humanos, bajo el respaldo de las Naciones Unidas, abarcan temas de gran importancia para los avances de las TIC, así como su aprovechamiento y su desarrollo al interactuar con el individuo, lo que resulta preocupante para las autoridades antes mencionadas, ya que el empleo indebido de las TIC (Tecnologías de Información y Comunicación) pueden llegar a vulnerar estos derechos. La información personal puede estar sujeta al escrutinio de terceros, por lo que se necesitan leyes y reglamentos para abordar estas situaciones, los riesgos para sus derechos y el uso de la información privada (Franco & Quintanilla, 2020).

En el cuerpo constitucional peruano, en su segundo artículo, numeral 6, se reconoce el derecho que tiene toda persona a los servicios informáticos, computarizados o no, de carácter público o privado, y que no afecten la intimidad personal y familiar.

En tal sentido, con el avance de la tecnología y el uso de las TIC, se deben implementar nuevos mecanismos y servicios que permitan a las empresas brindar a sus clientes la seguridad y protección de su información personal, sin embargo, la omisión de

estos mecanismos de seguridad digital ha generado preocupación en las personas ya que la información contenida en sistemas digitales puede ser filtrada por terceros, siendo usada con fines de lucro, vulnerando así la seguridad de sus datos personales, es así que encontramos el caso del delito de *SIM swapping*, que tiene como fin extraer información a través de la duplicación del *SIM*, para posteriormente acceder a la información contenida en el móvil y obtener un provecho ilícito, por ejemplo, realizar movimientos no reconocidos desde la banca móvil que se encuentra instalada en el equipo móvil sin consentimiento del titular.

Es, así que dentro de un marco constitucional se detallan los siguientes derechos los cuales son vulnerados ante la comisión del delito de *SIM swapping*:

3.1.1.1. El debido proceso

Este principio del derecho es adoptado por diversos Estados a fin de poder brindar seguridad jurídica a las personas, los principios generales del derecho están llamados a ser el fundamento primigenio de la norma y este en particular busca garantizar el respeto en la totalidad de los derechos de una persona que enfrenta un determinado proceso judicial; por lo tanto, en el marco jurídico nacional se encuentra establecido en el artículo 139 inciso de la Constitución Política del Perú.

Por otro lado, en cuanto a la conceptualización que surge en torno a este término existe el pronunciamiento del Tribunal Constitucional, quien emite una definición contundente en torno al presente instituto, sosteniendo lo siguiente: “El debido proceso está concebido como el cumplimiento de todas las garantías y normas de orden público que deban aplicarse a todos los casos y procedimientos existentes en el Derecho. (Sentencia de 16-10-12, emitida en el Exp. 0751-2002-AA-TC).

De lo citado anteriormente, se advierte que el principio del debido proceso significa una formalidad exigible y esencial para la preservación de un juicio justo, en los procesos llevados a cabo. En el caso del delito de *SIM swapping* en específico, se procura que este

proceso se celebre cumpliendo todas las garantías que este amerita, desde su etapa preliminar hasta su etapa final de juzgamiento, poniéndose en cuestión si verdaderamente existe un debido proceso en los casos de delitos informáticos, ya que es de conocimiento público que muchos de nuestros jueces y magistrados carecen de especialización en la materia y ello no exenta a la policía, que si bien es cierto no son administradores de justicia si contribuyen a las diligencias preliminares, en la que nuevamente se enfatiza el papel del juez y fiscal, en el extremo que en la mayoría de diligencias se exigen mandato judicial.

En el caso específico del delito de *SIM swapping*, donde al inicio de la investigación la Divindat pondrá en conocimiento al fiscal del caso los hechos denunciados y a través de una solicitud pedirá que este emita un requerimiento al juez para realizar el levantamiento del secreto bancario, que como ya se ha precisado en esta investigación es imprescindible para detectar al posible autor del delito y evitar que las evidencias sean alteradas o borradas. Sin embargo, ante el desconocimiento de los fiscales y jueces respecto a los escenarios en los que se desenvuelven este tipo de delitos, aunado a ello la carga procesal que padecen los órganos jurisdiccionales restan relevancia a la celeridad con la que deben tratarse el delito informático de *SIM swapping*.

La crítica surge en torno al escenario ya planteado, pues según el Conapoc a través de su diagnóstico multisectorial sobre la ciberdelincuencia en el Perú (2020) solo Lima y Arequipa (ciudad) tienen esta División Especializada de la Policía y solo Lima Metropolitana tiene una fiscalía especializada en registrar este tipo de delitos que vienen siendo desarrollados en medios informáticos. Por consiguiente, se precisa que el Estado viene trabajado en la creación de sectores del gobierno que tomen registro en estas tipologías de delitos; sin embargo, el avance del éxito de estas instituciones no está logrando surgir de la manera en que se tenía previsto; ya que es el centralismo, el principal factor que contribuye

con la ineficacia en los procesos seguidos en favor de la erradicación y/o lucha en contra de los delitos informáticos.

3.1.1.2. Tutela jurisdiccional en el delito informático *SIM swapping*

Previamente a explicar el derecho de tutela jurisdiccional efectiva, debemos partir por definir la tutela jurisdiccional, Priori (2003) señala que la tutela puede ser definida como la protección a un interés ante una situación en la que se siente lesionado.

Bajo esta premisa, Priori (2003) afirma que el derecho a la tutela jurisdiccional efectiva es aquel derecho que tiene toda persona con el fin de acceder al órgano jurisdiccional a efecto de solicitar protección ante una situación jurídica en la que se halle amenazada dentro de un proceso con mínimas garantías.

Por otro lado, la doctrina hace referencia a la relación entre tutela jurídica y tutela jurisdiccional, puntualizando que la tutela jurídica consiste en el reconocimiento de derechos que conllevan deberes correlativos; y la tutela jurisdiccional efectiva, es la función que tiene el Estado por intermedio de los jueces y los tribunales imponiendo sanciones ante la violación de una norma jurídica.

En este orden de ideas, el Tribunal Constitucional conforme la sentencia emitida en el Exp. N.° 763-2005-PA/TC de fecha 13 de abril del 2005, en su fundamento 6 en relación define a la tutela jurisdiccional efectiva se afirma lo siguiente: “Un derecho constitucional procesal en la que toda persona puede acceder a los órganos jurisdiccionales, independientemente del tipo de pretensión formulada y de la eventual legitimidad que pueda, o no, acompañarle a su petitorio”.

Se concluye que el derecho a la tutela jurisdiccional efectiva de toda persona que sea parte de un proceso penal donde se investigue un delito informático, como es el caso del delito de *SIM swapping*, es sumamente importante, ya que de esta forma al tener un bien jurídico lesionado puede la victima acceder al órgano jurisdiccional a fin de solicitar

protección; sin embargo, como es de verse actualmente frente a la falta de celeridad en las diligencias para esclarecer los hechos es probable que este derecho se vea quebrantado.

3.1.1.3. El derecho a la protección de los datos informáticos en el delito *SIM swapping*

Nuestra Constitución Política del Perú, conforme al artículo 2, numeral 6, establece que toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afectan a la intimidad personal y familiar. Siendo de esta manera, que este derecho no solo protege los datos físicos sino los contenidos en sistemas informáticos.

Para Chen Mork (2010), la protección a la información personal se fundamenta en garantizar directamente la adecuada protección y de manera indirecta el salvaguardar el derecho a la privacidad, honor, reputación, libertad de expresión, entre otros. Siendo ello que al estar constantemente en el avance tecnológico ha conllevado que este derecho se aplique al comercio electrónico, bastando que el consumidor solo navegue por la red, considerándose este un *SIM*ple acto como de consumo o comercio.

Actualmente, el avance de la tecnología y el comercio electrónico han creado una gran amenaza a la privacidad de la persona, poniendo en riesgo la información personal, tal es el caso que ante el acceso a una red se requiere que se proporcione cierta información personal no dándose explicación del porqué o el fin de estos datos; lo que origina de esta manera que los ciberdelincuentes ataquen los sistemas informáticos.

Centrándonos en el delito de *SIM swapping*, Contreras (2020) afirma que al encontrarse las evidencias en el ciberespacio se requiere un proceso especial para investigar por la misma naturaleza del delito, ya que, al utilizar medios informáticos, el sujeto activo se hace pasar por el titular de la telefonía móvil, teniendo acceso a la información personal contenida en correos electrónicos u otros para luego ingresar con estos datos a las cuentas

bancarias asociadas con el móvil y realizar retiros o transacciones bancarias por grandes montos de dinero, que causa un perjuicio económico al titular de la telefonía móvil.

Por lo que se denota de esta modalidad de fraude informático la forma en cómo operan los ciberdelincuentes quienes, a través del uso de herramientas tecnológicas, manipulan, alteran o eliminan información virtual contenida en dispositivos móviles que causa un perjuicio económico al titular, vulnerando el derecho a la protección de los datos informáticos.

3.1.1.4. El derecho a la autodeterminación informativa

La autodeterminación informativa implica que el titular pueda ejercer un control sobre la información relacionada con sus datos personales almacenados en bancos de datos o archivos públicos o privados, de manera que tenga acceso ininterrumpido a los datos y su modificación o supresión, o la solicitud de que pueda eliminar y evitar que terceros accedan a ella, cualquier tipo de operación sobre el mismo se realiza con su conocimiento y consentimiento.

Por otro lado, la autodeterminación informativa impone una serie de responsabilidades a las instituciones estatales y privadas que almacenan los datos; conforme a la Ley de Protección de Datos Personales (Ley N.° 29733) señala las facultades que le otorga al titular para ejercer sus derechos. Esta norma ha sido reglamentada mediante el Decreto Legislativo 1353 de fecha 7 de enero del 2017. De igual manera, mediante el proceso constitucional de hábeas data, establecido en el inciso 3 del artículo 200 de la Carta Magna, asegura la protección judicial del derecho a la autodeterminación informativa.

En tal sentido, el propósito del derecho de la autodeterminación informativa se basa en permitir el acceso completo de sus datos a una persona, la cual tendrá la libre disposición de hacer uso de esta y evitar que terceros accedan a ella a través de la tecnología informática

como sucede actualmente. En definitiva, la finalidad de este derecho fundamental es obtener un control sobre su propia información (Landa, 2017).

3.2. El convenio de Budapest

Este convenio se realizó ante el Consejo Europeo en el año 2001, el mismo que entró en vigor en el 2004. Teniendo como objetivo combatir el cibercrimen y los efectos del uso y desarrollo de las TIC. De igual manera, establece una política criminal común al nivel internacional que es responsable de brindar protección a la sociedad del aumento progresivo de los delitos cibernéticos en las últimas décadas, permitiendo a los Estados miembros establecer una legislación óptima que garantice una mejor cooperación internacional, facilitando la investigación, persecución y sanción tanto al nivel nacional como internacional.

De lo descrito anteriormente, el Tratado de Budapest (2001), se entiende como un instrumento legal de cooperación entre los Estados que lo conforman y los demás países firmantes, que tienen como objetivo lograr la protección de la sociedad frente a la "ciberdelincuencia"; de acuerdo con el Consejo de Europa-División de Ciberdelito se señala que el Convenio de Budapest cuenta con 68 estados parte y 9 estados que son miembros observadores y/o invitados.

Asimismo, la razón de ser de dicho convenio es optimizar la regulación interna de los estados miembros en materia de ciberseguridad, con mayor énfasis en materia penal, a fin de que sus organismos correspondientes puedan tener mayor capacidad para poder perseguir este tipo de delitos especiales (por ejemplo, fraude informático, interceptación ilícita, entre otros).

Objetivo

El objetivo principal de este convenio internacional es lograr una unión más estrecha entre los miembros, reconociendo también el interés de intensificar la cooperación de otros

Estados parte, proyectándose a través de una política penal común la protección de la sociedad frente a la ciberdelincuencia.

Del mismo modo, el convenio materia de estudio busca la prevención de todo acto que atente contra la confidencialidad, integridad y la disponibilidad de las redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos; proporcionando así la garantía de la tipificación, como delitos de dichos actos. De igual manera se busca la asunción de los poderes suficientes, para luchar eficazmente contra dichos delitos concretando así la facilidad en su detección, investigación y sanción, tanto a nivel nacional como internacional, sumado a ello establecer disposiciones materiales que contribuyan a una cooperación internacional rápida y fiable.

Estructura

El Convenio de Budapest cuenta con un preámbulo, despliega cuatro capítulos para dar tratamiento a los delitos informáticos, estableciendo diversas disposiciones para los Estados miembros, para ello desarrolló cuarenta y ocho artículos indistintamente, a modo de poder especificar diversos puntos emergentes ante la latente amenaza del crimen cibernético.

De acuerdo con la investigación planteada, el Convenio de Budapest desarrolla ciertos términos necesarios, para la comprensión de los delitos en mención:

Datos informáticos

Es un conjunto de símbolos que representan la información, las cuales permiten su procesamiento (Villazán, 2009). En pocas palabras es toda aquella información procesable por un dispositivo (computador, móvil).

Sistemas informáticos

Refieren las especialistas Prado y Nancy (2018), que estos sistemas no son más que un conjunto de elementos o *hardware*, que son necesarios para la explotación de aplicaciones informáticas o *software;* es decir; un sistema informático es tangible, susceptible de ser

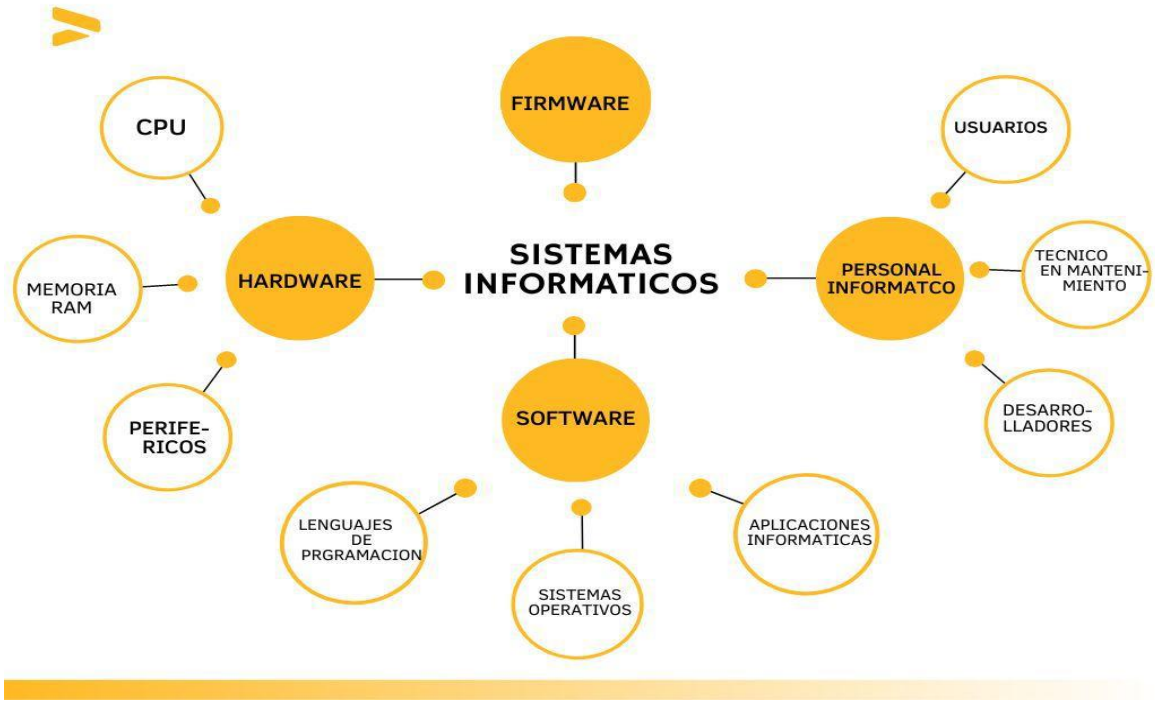
percibido por el tacto y por la vista (monitor, memoria RAM, teclado, unidad de proceso central, entre otros *SIM*ilares). En otro extremo tenemos a los programas y/o aplicaciones informáticas, los cuales forman parte del *software* y, por ende, son intangibles

Para una mejor percepción de la conceptualización prestada, el Dr. Villazán (2009, p. 10) indica que son cuatro elementos los que componen a un sistema informático, siendo los siguientes:

- Equipos (*hardware*-parte tangible)
- Programas (*software*-parte intangible)
- Firmware (*software* del sistema que reside en la memoria permanente de la computadora)
- Personal informático (representados por los usuarios del sistema informático, los desarrolladores y/o creadores de dicho sistema y el personal de mantenimiento)

Figura 1

Sistemas informáticos



Medidas que deberían adoptarse a nivel nacional

Consta de tres partes relacionadas con el derecho penal sustantivo, el derecho procesal y la justicia, que contienen las medidas que los Estados deben tomar para hacer efectiva la entrada en vigor del convenio; en particular, teniendo en cuenta la obtención, almacenamiento y presentación de datos informáticos en el marco del procedimiento y sus reglas de gobierno.

Sección 1. Derecho penal sustantivo

En cuanto a la primera sección, el Convenio de Cibercriminalidad (2001) incluye tipos penales estableciendo cuatro categorías:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos
- Delitos informáticos
- Delitos relacionados con el contenido
- Delitos relacionados con infracciones a la propiedad intelectual y los derechos afines.

Los delitos antes mencionados se desarrollan entre los artículos 2 y 10 del Convenio. Desde la fecha de su publicación en el 2001, se buscaba sancionar la conducta que perjudicaba la integridad de la información personal a través de la tecnología, tanto a personas naturales como jurídicas, sancionar explícitamente la difusión de pornografía infantil e infracción de la propiedad intelectual.

Sección 2. Derecho procesal

En relación con esta sección, el Convenio de cibercriminalidad (2001) prevé normas relativas al establecimiento de parámetros de obtención y conservación de pruebas que constan en las redes y sistemas, salvaguardando los derechos fundamentales de las personas, las cuales están destinadas a hacer exigibles el derecho procesal a fin de detallar distintas

medidas procesales para que los órganos investigadores puedan garantizar una investigación adecuada, de los delitos previstos en dicho convenio, entre las disposiciones comunes están las siguientes:

- Ámbito de aplicación de las disposiciones sobre procedimiento
- Condiciones y salvaguardas
- Conservación rápida de datos informáticos almacenados
- Conservación y revelación parcial rápidas de datos sobre tráfico
- Orden de presentación
- Registro y confiscación de datos informáticos almacenados
- Obtención en tiempo real de datos sobre tráfico
- Interceptación de datos relativos al contenido

La evidencia digital es más fácil de destruir y manipular a diferencia de la evidencia física; por lo tanto, la retención de datos es fundamental para el éxito de una investigación, por esta razón el convenio se enfoca en identificar maneras de asegurar evidencia digital para que pueda ser incluida en los documentos de investigación. Para tal efecto, la información deberá ser verificada y autenticada por las autoridades investigadoras, de manera que comprueben que los datos no han cambiado.

Sección 3. Jurisdicción

En la presente sección, el Convenio de cibercriminalidad (2001) señala la importancia y relación de la cibercriminalidad y la jurisdicción correspondiente, asados en los siguientes puntos:

- En el principio territorial
- En una variante del principio territorial
- En la base del principio de nacionalidad.

Donde cada estado miembro debe tomar medidas para confirmar esto, si delito se cometió y/o tuvo lugar en su territorio, si el hecho es castigado en su lugar de comisión o si ningún estado tiene jurisdicción sobre el territorio de este. Además, el acuerdo resuelve cualquier conflicto de jurisdicción, cuando múltiples partes invocan la jurisdicción en relación con un presunto delito descrito en dicho convenio.

Cooperación internacional (principios generales)

El Convenio de cibercriminalidad (2001) reconoce la importancia y necesidad de intensificar los vínculos de cooperación internacional para combatir la ciberdelincuencia, así como proteger el desarrollo de la tecnología en la información, tal como se desprende de los párrafos 7 y 8 del preámbulo:

Por lo que, el presente capítulo consta de dos secciones y está compuesta por: principios generales de la cooperación, y disposiciones específicas.

Principios generales

- Cooperación internacional: las partes cooperarán entre ellos aplicando instrumentos internacionales, tales como la cooperación internacional en materia penal y los acuerdos basados en la legislación la cual deberá ser recíproca que tengan como fin las investigaciones relacionadas a delitos donde están inmersos los datos y sistemas informáticos, así como obtener elementos informáticos de los delitos.
- Extradición: se aplicará siempre y cuando entre las partes exista la regulación de los delitos definidos en el artículo 2 hasta el 11 del Convenio en mención y su pena sea como mínimo de un año o una pena grave.
- Asistencia Mutua: este principio tiene como finalidad que las partes se presten ayuda mutua en las investigaciones o procedimientos en las cuales

estén inmersos los delitos informáticos o relacionados con datos o sistemas informáticos.

- Información espontánea: si bien es cierto entre las partes podrán comunicar información de sus propias investigaciones respecto a los delitos resaltados en este Convenio, también señala que las partes previamente a comunicar dicha información puede solicitar a la otra Parte que se proporcione la información de forma confidencial y bajo condiciones.
- Confidencialidad y restricción de uso: las partes podrán supeditar la comunicación de información cuando no se maneje de forma confidencial o se usen de otra manera las investigaciones contrario a lo pactado.

Disposiciones específicas

Dentro de esta sección, se resalta que las partes pueden solicitar entre ellas mismas la conservación de los datos informáticos de una forma rápida por medio de los sistemas informáticos que estén ubicadas en el territorio, así como prestar asistencia mutua con la finalidad del registro, acceso, confiscación u obtención de los datos informáticos.

Por otro lado, no se requerirá autorización de la parte cuando los datos almacenados sean de origen público, si existe el consentimiento lícito de la otra parte para revelarlo o tener acceso a los datos informáticos en otro Estado.

Otro punto para destacar, conforme el artículo 35, es que las partes designarán un punto de contacto, el cual estará activado las 24 horas de los 7 días de la semana a efecto de garantizar la asistencia inmediata en las investigaciones de los delitos donde están inmersos los datos y sistemas informáticos o para la obtención de pruebas.

Cláusulas finales

Este último capítulo comprende desde el artículo 36 hasta el 48, haciendo referencia que el presente Convenio estará sujeto a ratificación, aceptación o aprobación.

En lo referente a los efectos del presente convenio señala que el objeto es completar otros tratados, acuerdos multilaterales o bilaterales en las que participen las Partes.

3.2.1. Exigibilidad para el Perú

El Gobierno peruano, frente a los diferentes sucesos para erradicar la ciberdelincuencia, solicitó en el 2014 suscribirse al referido convenio, siendo aprobado por el Consejo Europeo en el 2015. Posteriormente, por Resolución Legislativa N.° 30913 del 2019, el Congreso aprobó el Convenio Budapest y, mediante Decreto Supremo N.° 10- 2019-RE del Poder Ejecutivo, fue ratificado entrando oficialmente en vigor el 01 de diciembre del 2019.

En ese sentido, el Perú asume el reto de mejorar su regulación interna en materia penal, solicitando apoyo y cooperación de otros Estados, ello en razón de la alta fragilidad de nuestro sistema digital, frente a los ataques cibernéticos o incluso enfrentar un escenario en el que los delincuentes digitales usen a la sociedad como fuentes de experimento para perfeccionar sus habilidades, ya que la regulación vigente padece de ciertas carencias en cuanto a su aplicación ejercida por los agentes de la justicia.

En lo que respecta a la exigibilidad, el Perú, al suscribirse y ser miembro del Convenio presentado, asumió el compromiso de luchar de manera efectiva contra la ciberdelincuencia y cooperar internacionalmente en el ámbito penal de manera oportuna y eficaz.

Frente al escenario planteado, el convenio expresa la potestad que tiene cada Estado para promover y concretar las medidas necesarias que sancionen a este tipo de delitos, que busquen la conservación rápida de la prueba, el establecimiento de procesos específicos en relación con los delitos informáticos, y demás medias *SIM*ilares. Conjuntamente, el convenio exhorta a los países miembros a aplicar las medidas necesarias para salvaguardar la conservación del secreto de ejecución en casos de custodia de datos y/o sistemas

informáticos, siendo estos los principales puntos de la cúspide de la problemática planteada en la presente investigación, ya que al apreciar nuestra norma Ley de Delitos Informáticos N.° 30171 (2014), y observar el proceder de los operadores de justicia, se encuentra ciertas falencias en la media en qué, en primer lugar, los delitos informáticos en específico el *SIM swapping* no son tratados con inmediatez, ya que la solicitud del levantamiento del secreto bancario implica un tratamiento riguroso por parte del fiscal y el juez. Puesto que, en este margen de tiempo, la conservación de la prueba corre riesgo de extinción o manipulación, desencadenando un posible fracaso en el resultado de dar con el autor intelectual, lo cual también va de la mano con el tipo de proceso que se lleva a cabo, pues los casos presentados han sido llevados como un proceso común u ordinario, sabiendo que este tipo de proceso tiene plazos no acordes con la naturaleza de estos delitos que exigen un enfoque especializado para su resolución.

Es así como se aprecia en la literalidad del artículo 16 inciso 3 del mencionado convenio se comprende una figura aplicable a la conservación de la prueba (datos informáticos y/o sistemas informáticos,) es la “custodia”; tomando como referente a este documento de índole internacional, consideramos a juicio propio que la medida de incautación, es una excelente alternativa que contribuiría a la agilización de la persecución del delito del *SIM swapping*, ya que no es imperiosa la decisión de un juez para su proceder.

Retomando el tema ligado a la exigibilidad para el Perú, se infiere que el presente convenio le otorga al Perú, como un Estado miembro, la potestad de poder dictar medidas que considere necesarias en favor de la prevención y sanción de los delitos informáticos, para ello expresa que este puede ser tomado como un modelo de referencia, sin embargo, no limita al Perú en basarse únicamente en las propuestas planteadas , por el contrario, motiva a sus miembros a que realicen una exhaustiva tarea en pro del bienestar de su población afectada por este tipo de delitos.

El Perú frente al llamado que hace el consejo europeo a través del convenio de Budapest ha buscado establecer distintas políticas que le permitan dar tratamiento a estos delitos, ya sea en las medidas preventivas como en las sancionadoras, para ello ha creado diferentes instituciones de apoyo, dentro de las cuales se encuentran las siguientes:

- La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (Dividant), siendo esta institución la encargada de las investigaciones de presuntos delitos informáticos (Diario "El Peruano", 2023).
- La Unidad Fiscal Especializada en Ciberdelincuencia, la misma que se encuentra en la ciudad de Lima, que es la única sede al nivel nacional pese al gran porcentaje de delitos informáticos que se registran diariamente en todo el país.
- La Coordinadora de Respuesta a Emergencia en Redes Teleinformáticas de la Administración Pública del Perú (PECERT) y la Presidencia del Consejo de Ministros, que tienen como misión coordinar la prevención, el tratamiento y la respuesta respecto a hechos cibernéticos en el sector público. Asimismo, se busca que elaboraren estrategias, prácticas y mecanismos necesarias con la finalidad de satisfacer necesidades de seguridad de la información del Estado (Romero, 2020).
- La Oficina Nacional de Gobierno Electrónico e Informático (ONGEI), cuya actividad está relacionada en la normativa informática, seguridad de la información, desarrollar proyectos en las TIC, entre otros.

3.2.2. Regulación de los delitos informáticos en el convenio sobre la ciberdelincuencia suscrito por el Perú

Los delitos informáticos se tipificaron inicialmente en el Código Penal de 1991, en el artículo 186, en el inciso 3; luego de una modificación en el Código Penal, estaban establecidas en el título V de delitos contra el patrimonio, capítulo X, entre los artículos 207-A al 207-C; pero en la actualidad este capítulo fue derogado y se creó una ley especial para este tipo de delitos.

Dicha ley de delitos informáticos (Ley 30096, 2013), contempla 7 capítulos que se encuentran estructurados de la siguiente manera: en el capítulo I, se menciona el propósito y objeto de la ley, estableciendo conforme al derecho procesal penal de cada país los mecanismos necesarios para la investigación y el procesamiento de dichos delitos mediante el uso de un sistema informático. Asimismo, en el capítulo II, se hace mención de los delitos contra datos y sistemas informáticos, en los cuales se ve vulnerado el acceso a los datos de los sistemas informáticos. Por su parte, en el capítulo III, se tipifican los delitos contra la indemnidad y libertad sexual. También, en el capítulo IV se señalan los delitos informáticos contra la intimidad y el secreto de las comunicaciones, sobre la interceptación de datos informáticos. Además, en el capítulo V, se encuentran los delitos informáticos contra el patrimonio, como el fraude informático que se considera como un delito de resultado, porque no basta con la realización de la conducta exigida en el delito mencionado, sino que es necesario un resultado posterior que consiste en causar un daño o perjuicio a un tercero. Mientras que en el capítulo VI, se hace mención a los delitos informáticos contra la fe pública, siendo que para la realización de este ilícito se cause un daño como resultado del hecho. Y, por último, y no menos importante tenemos el capítulo VII, sobre las disposiciones comunes, en el cual se alude al abuso de mecanismos y dispositivos informáticos.

Posteriormente, se promulgó la Ley N.° 30171 (2014), modificando a la ley señalada precedentemente. El propósito de esta fue adaptar la anterior ley a los estándares legales del Convenio de Ciberdelincuencia, siendo las modificatorias las siguientes: en el artículo 1, se realizaron modificaciones de los artículos 2, 3, 4, 5, 7, 8 y 10. Además, en el artículo 2, se ejecutó la modificación de la tercera, cuarta y undécima disposiciones complementarias finales. Mientras que en el artículo 3, se da la incorporación del artículo 12 en la presente ley. A su vez, en el artículo 4, se modificaron los artículos 158, 162 y 323 del Código Penal. Y, por último, en el artículo 5, se incorpora al Código Penal los artículos 154-A y 183-B; y la Única Disposición Complementaria Derogatoria, deroga el artículo 6 de la Ley 30096, Ley de Delitos Informáticos.

3.3. Obligaciones por parte del Perú para la persecución penal efectiva de los delitos informáticos

El Perú, al suscribirse al Convenio de Budapest con fecha 12 de febrero del 2019 mediante la Resolución Legislativa N.° 30913, adopta el compromiso de combatir juntamente con la comunidad internacional la persecución y prevención de los delitos informáticos.

No es algo novedoso que los delitos hoy en día por sus múltiples modalidades y formas cibernéticas actúen en territorio nacional, lo que ha conllevado que el Perú adopte medidas legislativas, las mismas que en el trayecto resulten óptimas para coadyuvar con las investigaciones en materia penal donde estén vinculados los delitos informáticos; tal como lo señala el artículo 13 del Convenio sobre la Ciberdelincuencia donde el Perú es parte de este tratado internacional.

Por lo que, ante los diversos delitos cibernéticos, la persecución penal a cargo del Ministerio Público como titular de la acción penal ha conllevado una visión estratégica con el fin de luchar contra la ciberdelincuencia. En tal sentido, esta entidad autónoma es un

instrumento jurídico en el que los fiscales y jueces realizan requerimientos internacionales, tales como la cooperación internacional y la asistencia mutua vinculados a los ciberdelitos, los cuales se encuentran regulados en la Ley N.° 30171, Ley de Delitos Informáticos, y ha tomado diferentes decisiones para la persecución penal efectiva.

En tal sentido, el Ministerio Público, como organismo constitucional autónomo del Estado, ha desarrollado diferentes guías y manuales con la finalidad de uniformizar la investigación en el proceso penal vinculado a los delitos informáticos, así como la recolección y preservación de elementos digitales que estén vinculados a los ciberdelitos.

Dentro de ellos, se tiene a los siguientes:

- Guía de Análisis Digital Forense del Ministerio Público (2020, Ministerio Público), la cual fue aprobada con fecha 11 de agosto del 2020 mediante Resolución de Gerencia General 365-2020-MP-FN-GG, cuyo objetivo es delimitar procedimientos para estandarizar la labor pericial a cargo del Área de Análisis Digital Forense en las evidencias digitales que están inmersas en procesos de investigación fiscal.
- Manual de Recojo de Evidencia Digital (Ministerio del Interior, 2020), la cual fue aprobada mediante RM. N.° 848-2018-IN por el Ministerio del Interior, la cual es una herramienta para la PNP que ante su aplicación podrá recabar y preservar el recojo de dispositivos que almacenen datos que estén relacionados con el hecho delictivo, de esta manera no se contaminará, suprimirá o alterará al objeto del delito, ya que se realizará de una forma profesional.
- Manual de Evidencia Digital, (MINJUSDH, 2017), que fue elaborado en el 2017, por el Ministerio de Justicia y Derechos Humanos juntamente con la American Bar Association, cuyo objetivo es guiar la actuación del personal

policial y fiscales que se encuentren ante un delito donde se hallen dispositivos de almacenamiento informático para su posterior investigación penal.

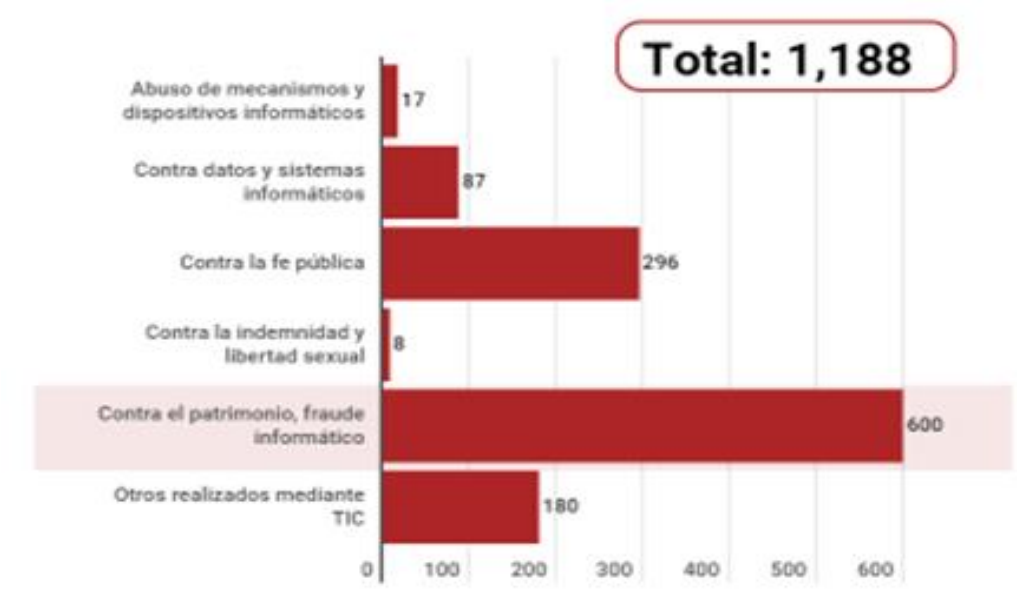
En tal sentido, el Estado peruano ha realizado diferentes guías y manuales con el fin de actuar de una forma eficaz ante la investigación penal en los delitos informáticos que tienen una especialidad en el objeto del delito, ya que los datos y sistemas informáticos o aquellos dispositivos que contengan información digital son fáciles de manipular o alterar, es por ello, que ante la aplicación de estas guías, se establece una uniformidad en el proceso a fin recabar aquellos instrumentos digitales de una forma profesional y así no dejar que estos hechos ilícitos queden impunes.

Por otro lado, se tiene la labor presidida por la PNP, a través de la Divindat de la Dirincri, que de forma conjunta con el Ministerio Público ejercen una labor importante en las investigaciones vinculadas a los delitos informáticos.

Conforme a la estadística señalada por el Ministerio Público, se tiene que en el 2021 se registró 18,596 denuncias por delitos informáticos, que se incrementaron un 92.9% frente al 2020. En palabras del coronel Erick Ángeles, jefe de la Divindat, los ciberdelincuentes operan bajo el uso de redes sociales, sitios web, correos electrónicos y mensajes de delitos (Diario Oficial El Peruano, 2021)

Figura 2

Denuncias recibidas en la Divindat de enero a abril del 2021



Es así que el Perú no es ajeno a las diferentes modalidades de ataques cibernéticos, destacándose del presente gráfico, que el gran porcentaje de delitos informáticos son contra el patrimonio en la forma de fraude informático.

3.3.1. Lineamientos normativos del delito informático *SIM swapping*

Aunque la norma peruana no expresa de manera literal los principios bajo los que se rige, se infiere que esta comparte los fundamentos que se promueve en el Convenio de Budapest y que este expone de manera literal.

De los principios que se mencionan, encontramos los siguientes:

- Principio de cooperación internacional. Este principio que resulta base fundamental de la concepción del Convenio de Budapest guarda relación con nuestra norma. En el extremo que refiere el compromiso asumido por el estado peruano, al firmar y ratificar convenios multilaterales; a fin de consolidar una colaboración activa con la comunidad internacional, todo ello debido a contener el avance acelerado de estas actividades delictivas y

preservar de este modo la seguridad jurídica que todo estado tiene la obligación de tutelar.

- En cuanto al principio de asistencia mutua y el principio de información espontánea, ambos guardan una estrecha relación, si bien es cierto el primero incentiva a que los Estados miembros se apoyen en las etapas de investigación y en sí durante el proceso en el que se ven inmersos este tipo de delitos. El segundo principio nos advierte que la manipulación de información que de pronto se requiera de una parte para con la otra podrá hacerse en los términos que estas acuerden, es decir, si se desea compartir información de manera confidencial podrá hacerse sin ningún tipo de impedimentos, ya que recordemos que este convenio busca un trabajo arduo en el que los países miembros actúen en un marco de fraternidad con un objetivo común. En relación con la norma nacional, estos principios actúan como rectores en la actuación del Perú como un estado miembro y en cuanto a una interpretación en el ámbito nacional podríamos a opinión propia asegurar que estos principios se relacionan con una de las disposiciones complementarias que la ley expresa para regular la actuación de las autoridades esto en un marco nacional. Es decir, tenemos en claro que los principios desarrollados en líneas precedentes actúan y cumplen con su propósito, pero si quisiéramos darle un enfoque nacional, podríamos observar que esta colaboración que se promueve involucra a una serie de agentes intervinientes tales como la Fiscalía y la Policía Nacional, siendo estos últimos quienes asisten al ministerio público en un una primera fase de la etapa preliminar de la investigación de dichos delitos.

Como se observa, los principios bajos los cuales se rige el convenio contra la ciberdelincuencia adoptan la fiel postura de impulsar las buenas relaciones entre sus estados miembros, para consolidar una colaboración eficaz, en este extremo se valora la labor que viene desempeñando España en su persecución del delito del *SIM swapping*, y en general de los delitos informáticos que vienen lo que genera una fuerte inseguridad en la sociedad, bajo esta premisa aunque en el Perú no se haya registrado un caso de extraterritorialidad en relación al *SIM swapping*. No somos ajenos a la concepción de que dicha propuesta si es posible y ha sido desarrollada en países del continente europeo, tales como España y Rumania e Italia, que en un trabajo conjunto con la Europol lograron desarticular una banda dedicada a la comisión del delito de duplicación de *SIM swapping.* Asimismo, cabe destacar el papel que desempeñaron los analistas de la Policía Nacional de Italia, quienes prestaron colaboración fundamental para el éxito de esta operación a la cual se le atribuyó el nombre de "Quinientos Ducim" (Naked Security, 2020), la misma que sirvió como ejemplo en Austria, en donde la colaboración de Rumania nuevamente se hizo presente. Por tanto, los casos presentados han llevado su debido proceso de investigación y juzgamiento apreciándose el éxito de ambas etapas y probablemente ello se deba al trabajo solidario de las naciones mencionadas, a fin de lograr brindar una mayor seguridad jurídica a sus gobernados.

3.3.2. Medidas procesales aplicables al delito de *SIM swapping*

El Convenio de Budapest menciona que los Estados podrán adoptar diferentes medidas legislativas o de otra índole que resulten indispensables para conocer los procedimientos que exigen este tipo penal y los demás que se incluyen dentro de este convenio. Para ello, la norma adjetiva peruana a través del derecho a la cautela o de la tutela plena de las sentencias, busca promocionar el aseguramiento efectivo de esta última a futuro; en tanto se tramita el proceso principal, es exclusivamente de carácter procesal, así mismo

este procedimiento cautelar goza de autonomía y puede solicitarse tanto en proceso contenciosos como no contenciosos.

De conformidad con lo expuesto para el caso en concreto del *SIM swapping*, no solo recae sobre la figura del levantamiento del secreto bancario, sino también en la posible aplicación de la incautación, siendo esta el principal planteamiento de la investigación presentada, ello en relación con la obtención de una respuesta rápida con óptimos resultados en la preservación de la prueba.

En relación al levantamiento del secreto bancario, al ser una medidas limitativa de derechos, que recae justamente en derechos fundamentales, requiere de la autorización del juez competente para resolver este tipo de delitos, conjuntamente con esta medida, la incautación se presenta como una alternativa que busca la preservación de la prueba actuando con mayor rapidez cuando se esté frente a un caso de flagrancia o peligro inminente de su perpetración (...) contemplado en el artículo 218 inciso 2 del Código Procesal Penal peruano, situación donde la norma nos indica que el agente policial podrá incautar el bien sin necesidad de autorización del fiscal o judicial.

Seguidamente a modo de conclusión se prevé que las dos figuras anteriormente desarrolladas forman parte del compromiso de generar medidas legislativas y *SIM*ilares que contribuyan con la prevención y la sanción a los tipos penales que versan en el convenio de Budapest.

a) Ámbito de aplicación de las disposiciones de procedimiento

Como preámbulo al desarrollo de este punto, se encuentra la premisa citada anteriormente “Los estados parte adoptarán medidas legislativas y de otro tipo que resulten necesarias (...)” (Convenio de Budapest, 2001); en relación con lo que establece cada artículo en particular, se interpreta que, en este caso el Perú deberá adoptar aquellas medidas

legislativas y de otra índole que crea pertinentes para determinar los poderes y procedimientos aplicados en la investigación penal.

De acuerdo con la interpretación de lo establecido en la norma peruana en relación con el convenio de Budapest, se determina, que la norma procesal alberga la figura de la incautación, aplicable al *SIM swapping* en favor de una investigación con mayor éxito en la persecución del autor intelectual, figura procesal que además brinda una mayor participación del agente policial en el caso determinan de flagrancia y cuando se prevea peligro en sus perpetración, resultando una contribución mayor en la investigación y por tanto una posible mayor eficacia en la conclusión de los procesos a los que son sometidos los delitos en mención.

b) Conservación rápida de datos informáticos almacenados

Aunque en el Perú no se encuentre establecido, de manera expresa, el proceso aplicado a este tipo de delitos, a diferencia de lo establecido en la normal chilena, es importante recalcar que en un proceso penal común donde se investigue un delito informático; la ley peruana actúa de acuerdo con ciertos plazos establecidos, los cuales no resultan lo suficientemente idóneos para la recolección de datos informáticos, siendo que a criterio del grupo de investigación se considera que los plazos para este tipo de procesos atenta a la conservación de la prueba por tratarse de un proceso común, por ello, es posible resguardar la prueba como tal aplicando la figura de la incautación, de este modo podría llevarse una investigación a profundidad reduciendo la alteración, modificación y/o supresión de la prueba (datos).

3.4. Alcances de la medida de incautación como instrumento procesal de búsqueda de pruebas y limitación de derechos

La medida procesal de la incautación es la apropiación o posesión de bienes por parte de una autoridad, estos bienes se cree que constituyen el objeto o el producto de un delito

que se investiga, garantiza que dichos bienes u objetos no desaparezcan y sirvan como medios de prueba para el esclarecimiento de los hechos, evitando el entorpecimiento de la búsqueda de la verdad.

En el Código Procesal Penal se encuentra como instrumento procesal la incautación, la cual forma parte esencial en un proceso penal y tiene sustento dentro de nuestro ordenamiento jurídico.

Cáceres (2008) menciona que la incautación comprende en el apoderamiento forzoso por parte del fiscal de los objetos o instrumentos del delito con los que se hubiere ejecutado el acto delictivo, así como los efectos, sean estos bienes, dinero, ganancias o cualquier producto procedente del delito, así se encuentre en posesión de personas naturales o jurídicas.

La legislación del Perú en relación con el Acuerdo Plenario N.° 05-2010/CSJ-116 establece que la incautación tiene una estructura dual: como medida de coerción en los artículos 316º al 320º (permite asegurar las fuentes de las pruebas materiales), y como medida de búsqueda de pruebas y restricción de derechos en los artículos 218º y 223º (previene el ocultamiento de bienes, respecto a la obstaculización de la averiguación de la verdad), previstos en el Código Procesal Penal. En ambos casos, la incautación funciona como un acto emitido por una autoridad que restringe la propiedad de bienes o cosas de alguna manera relacionado con delitos penales.

El propósito de esta medida se pretende resguardar los bienes empleados o vinculados a la investigación de un hecho delictivo. En este caso, el fiscal podrá solicitar al juez de Investigación Preparatoria la incautación de los bienes u objetos relacionados al delito. La solicitud deberá demostrar que el uso del bien agravaría, perpetuaría o facilitaría la comisión del delito. Como parte de esta diligencia, el fiscal ordenará registrar, detallar, asegurar e inventariar los bienes, precisándose que lo mencionado deberá quedar registrado

en un acta, consignándose fecha y hora, y firmada por los participantes y testigos. Del mismo modo, deberá señalarse el responsable de la custodia, administración y destino final del bien. Se proporcionará a cada uno de los afectados una copia certificada.

Esta medida tiene como objetivo adquirir y proteger bienes utilizados relacionados con el delito. En este caso, el fiscal, como persecutor de la acción penal, podrá solicitar la incautación de bienes relacionados al delito ante el juez de Investigación Preparatoria. Dicha petición debe demostrar que la libre disposición de los bienes agravaría o facilitaría un delito penal.

3.4.1. Límites constitucionales a la medida de incautación de bienes

Conforme a la regulación constitucional, al adoptar las medidas procesales de coerción real, estas de cierta forma limitan derechos fundamentales que como persona son inherentes.

San Martin (2020) señala que en la medida procesal de incautación de documentos privados, contables y administrativos se ve limitado el derecho al secreto y la inviolabilidad de documentos privados, tal conforme a lo regulado en el artículo 2 de nuestra Carta Magna inciso 10. Esto debido a que al ejecutarse esta medida procesal mediante el recojo de las evidencias que estén inmersas en el hecho punible como objeto del delito y sirvan como elementos de convicción para contribuir a la investigación; se ven afectados, ya que los documentos pasarán a ser custodiados para el esclarecimiento de los hechos no habiendo opción que el titular del bien pueda dar uso de estos.

Por lo que, conforme a lo señalado por el autor si bien es cierto se transgrede el derecho al secreto y a la inviolabilidad de documentos de carácter privado, en el caso en concreto del delito de *SIM swapping*, los documentos digitales contenidos en soportes informáticos o sistemas informáticos son de carácter privado, en tal sentido, ante un posible delito de fraude informático se ve limitado el derecho a la inviolabilidad de documentos

privados; siendo que el fiscal para esclarecer los hechos, adopta la medida de incautación de bienes a fin de poder recabar las evidencias digitales.

Cabe precisar que dentro de la afectación a los derechos que produce la medida de incautación, también encontramos como eje central al derecho de propiedad, donde se evidencia la restricción al derecho del titular del bien (equipo móvil y/o portátil), el cual contiene la información digital, que constituye la consolidación de la prueba, en este extremo solo nos referimos al cambio de dominio del bien el cual pasará a ser custodiado por la Policía Nacional del Perú.

Por lo tanto, aunque se vea limitado el derecho a la inviolabilidad de documentos privados y el derecho a la propiedad, se precisa que la medida de incautación de bienes tiene una base legal, la cual se funda en el esclarecimiento de los hechos y para su aplicación es necesario verificar la necesidad de la medida y si esta es proporcional para el caso.

En conclusión, al configurarse la incautación existe la privación del dominio y como consecuencia deviene en una desposesión provisional que cesará cuando las razones que motivaron la medida ya no sean necesarias.

3.4.2. Tratamiento normativo de la incautación de bienes en el ordenamiento jurídico peruano.

a) Medida instrumental restrictiva de derecho

En el ordenamiento jurídico, conforme el artículo 218 del Código Procesal Penal nos indica que la medida instrumental restrictiva de derecho tiene como principal función conservar y asegurar las fuentes de prueba material, para luego ser utilizadas como medios probatorios y permitan el esclarecimiento de los hechos investigados.

Según lo señalado por San Martín (2020) respecto a la incautación como medida instrumental, indica que el bien debe ser el cuerpo del delito o las piezas de convicción, es

decir la relación existente entre el tiempo, medio y objeto de investigación que permitirán el esclarecimiento de los hechos del delito

b) Medida de coerción cautelar

Conforme la normativa procesal, se tiene que la medida de incautación puede ser de carácter cautelar la misma que se encuentra prevista desde el artículo 316 al artículo 320 del Código Procesal Penal, siendo que esta medida recaerá sobre bienes que son fuentes de prueba u objetos de decomiso.

San Martín (2020) hace una clara distinción entre la medida de incautación instrumental y la medida de incautación cautelar, siendo que la medida de incautación de carácter cautelar sus efectos deben ser a consecuencia de una infracción penal, así como los instrumentos, los efectos o ganancias del delito. Asimismo, señala que la incautación cautelar restringe el derecho a la propiedad a raíz de la comisión del hecho ilícito y la relación entre el bien o activo y la conducta atípica.

Finalmente, esta medida procesal es aplicable en las primeras diligencias, no descartando la posibilidad de que se realice en el transcurso de la investigación preparatoria presidida por el Ministerio Público y la Policía. En el caso que haya peligro en la demora, el fiscal a cargo ordenará que se realice la incautación para posteriormente solicitar la resolución de confirmatoria ante el juez de Investigación Preparatoria, ante la ausencia de este presupuesto, es decir, peligro en la demora, se requiere la resolución cautelar para la aplicación de esta medida procesal

3.4.3. Jurisprudencia respecto a la medida procesal de incautación de bienes

a) Recurso de Casación 864-2017, Nacional, de fecha 21 de mayo del 2018, por la Sala Permanente de la Corte Suprema de Justicia de la República, en la que se emite pronunciamiento respecto a la medida cautelar de incautación, destacándose lo siguiente:

Conforme al fundamento sexto de la sentencia, señala que la medida cautelar puede ser de dos tipos: medida de coerción real o patrimonial, todo ello conforme el artículo 316 numeral 1 del Código Procesal Penal. Asimismo, indica que esta medida procesal el objeto material incide en las consecuencias del ilícito, en los instrumentos que se usaron para la ejecución y los objetos permitidos en un ámbito legal; sin embargo, conforme el numeral 3 del citado artículo habla respecto a las ganancias del delito.

Por otro lado, la incautación se caracteriza por ser una medida limitativa del derecho a la propiedad, la misma que se aplicará siempre y cuando concurran estos requisitos:

La intervención indiciaria, es decir, que se encuentran suficientes elementos de convicción.

Principio de proporcionalidad: idoneidad, necesidad y estricta proporcionalidad. Conforme, el artículo 253, numeral 2 y 3 del Código Procesal Penal señala que el principio de proporcionalidad desde un punto de vista de coerción real se aplica a fin de evitar riesgos de ocultamiento, obstaculización en el proceso para averiguar la verdad o insolvencia sobrevenida.

Sin embargo, si nos referimos a la medida de incautación cautelar, el peligro de esta medida se aplica para neutralizar el peligro, conforme el artículo 317, numeral 1 del Código Procesal Penal. Respecto a los suficientes elementos de convicción abarca no solo la atribución del hecho punible al imputado sino también el riesgo de ocultamiento patrimonial de los bienes involucrados en el hecho delictivo o el peligro de reiterar el hecho delictivo utilizando de diferentes modos, o de forma específica los que puedan agravar o prolongar las consecuencias del delito o cometer otros delitos.

Conforme el fundamento sexto, la Sala Penal Permanente señala que la medida de incautación cautelar se aplicará en los bienes vinculados a los delitos, ya sea aquellos bienes que estén en su poder haya o no intervenido en el delito, de ser aquella persona que no haya

sido responsable del ilícito, el tercero debe ser de mala fe, solo así se podrá incautar y luego el decomiso. Sin embargo, se resalta que el decomiso no se dispondrá cuando el bien delictivo haya sido transferido a un tercero de buena fe y a título oneroso, todo ello conforme al artículo 102, último párrafo del Código Penal.

En tal sentido, el adquiriente de buena fe tiene la condición de tercero en el proceso penal por lo que se autoriza la participación en el proceso, así como oponerse a la incautación, conforme el artículo 318, numeral 4 del Código Procesal Penal.

Otro de los puntos importantes en este pronunciamiento, es respecto al bien delictivo, ya que es factible que con posterioridad al hecho delictivo se haya transferido a un tercero, en estos casos lo importante es las condiciones en la cual este tercero adquirió o hizo posesión del bien, en tal sentido, solo procederá la incautación si no actuó de buena fe.

Finalmente, en la medida de incautación lo importante es que el bien afectado lleve un control, ya sea por la persona que tiene la posesión o su inscripción en SUNARP; sin perjuicio, del decomiso del bien el cual será trasladado a la titularidad del Estado. En el caso del decomiso, es una consecuencia accesoria no respondiendo a la responsabilidad pecuniaria a consecuencia del delito; por el contrario, la incautación prohíbe ante su inscripción que se realice transferencias o gravámenes por el afectado, recalcándose nuevamente que, conforme el artículo 318, numeral 3 del Código Procesal Penal hace referencia al afectado dejando claro que puede ser o no el imputado; precisando, que el afectado es aquella persona que tiene poder sobre el bien.

b) Acuerdo Plenario N.° 5-2010/CJ- 116, de fecha 16 de noviembre del 2010, mediante el VI Pleno Jurisdiccional de las Salas Penales Permanente y Transitoria teniendo como asunto principal la medida procesal de la incautación. De la misma se destaca, una definición respecto a la incautación al referirse como una medida procesal la cual puede ser: una medida instrumental restrictiva de derechos prevista en el artículo 218 al 223 del Código

Procesal Penal o una medida de coerción prevista en el artículo 316 al 320 del mismo del cuerpo normativo. En el supuesto de la incautación como medida instrumental, esta va recaer:

- Sobre bienes que constituyen cuerpo del delito, es decir, aquel contra el que va a recaer el hecho punible o haya sufrido los efectos lesivos, pero de una forma directa,
- Cosas que se relacionen con el delito que sean útiles para el esclarecimiento de los hechos materia de investigación, es decir, los medios u objetos con los cuales se llevó a cabo la comisión del delito.

Conforme al artículo 316 inciso 1 del Código Procesal Penal, la incautación cautelar incide en lo siguiente:

- En los efectos por la acción delictiva, es decir, los objetos o ventajas patrimoniales derivadas del hecho delictivo.
- Los instrumentos que formaron parte para su ejecución, es decir, aquellos objetos que ante su uso ya sea como medio o fin han servido para la ejecución del hecho delictivo.
- El objeto del delito, son las cosas materiales sobre las que recayó la acción típica.

Por otro lado, la incautación ya sea instrumental o cautelar será realizada por la Policía o la Fiscalía en primer término; sin embargo, para su confirmatoria se necesita la decisión del juez de Investigación Preparatoria. En tal sentido, se presentan los siguientes supuestos: En los casos de flagrancia delictiva o peligro inminente conforme el artículo 259 del Código Procesal Penal, la Policía debe incautar todos los bienes relacionados con el hecho punible, a efecto de garantizar su probanza efectiva.

Si no se dan estos supuestos, la incautación se realizará como una de las primeras diligencias en la etapa de investigación preparatoria; para este caso, el policía requiere de la autorización del fiscal. Por lo que la decisión judicial será requisito para la incautación siempre y cuando no haya un peligro por la demora y esta no recaiga sobre bienes de decomiso, es decir, se aplicará la medida procesal por orden judicial cuando no haya riesgo en desaparición del bien.

En tal sentido, el grupo de investigación concluye que, ante la aplicación de la medida procesal de incautación, el juez de la Investigación Preparatoria debe dictar aprobando o desaprobando la confirmatoria de incautación instada ya sea por el fiscal o la Policía, la cual debe solicitarse inmediatamente. Asimismo, ante el requerimiento de incautación no se exige la celebración de una audiencia solo basta correr traslado previo a los sujetos procesales en especial al afectado siempre y cuando no exista riesgo fundado de la pérdida de la medida.

3.4.4. Bienes susceptibles de incautación

Para indicar los bienes susceptibles de incautación, es necesario esclarecer la dualidad que recae sobre esta medida procesal, como medida de búsqueda de pruebas y restricción de derechos (instrumental) desarrollada en los artículos 218° al 223° del Nuevo Código Procesal Penal y finalmente tomada como una medida de coerción en el extremo que evita la prolongación de los efectos lesivos del delito, dicho de otro modo su aplicación permite prevenir la ejecución de consecuencias pecuniarias (cautelar).

La incautación recae sobre todo bien que sea objeto y/o instrumento del delito, tratándose del delito de *SIM swapping* recaerá sobre los datos almacenados por parte del autor del delito, cabe mencionar estarían catalogados como un bien mueble intangible, así mismo, de ser necesario se incautarían los equipos que fueron objeto para la consumación del tipo penal (teléfono móvil, computador portátil, CPU, etc.).

3.4.5. ¿Puede aplicarse la incautación de datos informáticos?

La incautación, secuestro o congelamiento de bienes es una medida cautelar que se puede aplicar dentro de un proceso penal con el fin de esclarecer los hechos. Para ello, deben respetarse los protocolos a fin de poder conservar la prueba del delito puesto que cabe la posibilidad que estos bienes sean devueltos a su titular en caso de que la sentencia no disponga el decomiso o, si lo decreta, hacer efectiva la ejecución.

Bajo esta premisa, se observa que en la legislación peruana no se establece la aplicabilidad de la medida de incautación sobre los datos y/o sistemas informáticos, lo que conlleva a sostener la afirmación que; si es aplicable esta medida, bajo el criterio adoptado en legislaciones internacionales.

Por ejemplo, en el caso de Chile conforme a su legislación penal, regula un tratamiento del levantamiento de la evidencia de los hechos denominado "cadena de custodia", la cual va a permitir la conservación de la evidencia, es decir, la confiabilidad y seguridad de las pruebas recogidas para el esclarecimiento de los hechos.

Si bien es cierto, la finalidad de esta medida consiste en que ante su aplicación, el juez tenga asegurada que la evidencia presentada en la corte sea la misma hallada en el lugar de los hechos; no obstante, se observa que no existe una norma legal o reglamentaria que establezca la manera de cómo se debe procesar, almacenar y analizar la evidencia incautada en la escena del crimen, pero existen diferentes etapas en la cadena de custodia por los cuales se puede evidenciar inmutabilidad de las pruebas.

Conforme a la legislación chilena respecto a la incautación de bienes, establece 4 etapas: a) el hallazgo y resguardo de los hechos: bienes materiales y/o sujeto que realizó el ilícito, para obtener indicios importantes para la investigación; b) inspección preliminar y búsqueda de los indicios, esta etapa está a cargo de la policía, cuya labor primordial es el recojo y conservación de objetos que son utilizados como medio de prueba; c) fijación de la

huella o evidencia: permitirá la determinación exacta de la ubicación y estado de los indicios que son de importancia para la investigación, en esta etapa se puede disponer o hacer uso de aparatos tecnológicos para la toma de fotos o filmación, croquis y acta; d) la recolección y embalaje de la huellas o evidencias; para luego hacer el traslado y la entrega de la evidencia y de esa manera proceder con la custodia; dichas etapas se encuentran en la legislación establecida en el Código Procesal Penal chileno, las cuales son aplicables de manera general en relación con los ilícitos desarrollados en el Código Penal como son los delitos comunes.

Ahora, bajo el análisis efectuado en dicha legislación sobre el tema de la cadena de custodia, y enfocándose en el contexto de la incautación de los datos informáticos, la policía realiza lo que es "un resguardo especial" que es aplicado en la evidencia electrónica, es decir, si bien es cierto son aplicables las etapas de la cadena de custodia; se debe tomar en cuenta que para este tipo de evidencia se tiene que probar el cumplimiento de resguardos especiales y de esta manera poder asegurar que el material obtenido no sea alterado o destruido (Santelices, 2014).

Al referirse a un resguardo especial, existe cierta complejidad a la aplicación de esta medida en los delitos informáticos porque surge la dificultad al delimitar con certeza el lugar exacto de los hechos y el material de prueba o los objetos utilizados para la realización del ilícito, debido a que se requiere del uso de un medio tecnológico y de una conexión de internet; dichos datos resultan ser volátiles pero a la vez permiten obtener indicios para la investigación si estos son incautados a tiempo, es decir, si los dispositivos de almacenamiento electrónico, en general sobre la información contenida en los mismos, correos electrónicos, entre otros (*software*) y la evidencia física que esté asociada a la electrónica (*hardware*) y que contenga información de interés para la investigación.

Por otro lado, tenemos la legislación de la provincia de Río Negro, Argentina, resaltándose que la medida de incautación si tiene aplicación en el delito informático,

conforme al artículo 148 de la Ley N.° 5020 promulgada en el 2014, señala que cuando se secuestren datos o equipos informáticos se procederá conforme a lo previsto para los documentos, siendo así que el examen de estos se hará bajo responsabilidad del fiscal.

En la misma línea, el Código Procesal Penal de la Nación Argentina señala en su artículo 144 (incautación de datos), que el juez, a pedido de parte o auto fundado, puede ordenar el registro de un sistema informático o parte de este, medio de almacenamiento de datos informáticos o electrónicos, cuyo objetivo es secuestrar los componentes del sistema, obtener copia o preservar los mismos. En este caso, el examen estará a cargo bajo responsabilidad de quien lo solicitó.

En tal sentido, se puede apreciar que el Código Procesal Penal permite la aplicación de la figura de la incautación en la investigación y adquisición de material probatorio de índole informático o electrónico para el eventual juzgamiento y sanción de los delitos informáticos.

Bajo este arduo análisis de la aplicación de la medida de incautación de bienes informáticos en la legislación comparada (Chile y Argentina), es sumamente importante que en la legislación peruana se regule esta medida procesal, ya que bajo el registro y secuestro de datos los cuales se encuentran en soportes digitales y/o informáticos, serán parte de la prueba trascendental en un proceso penal, desvinculándose que no solo resulta necesario la evidencia física sino la evidencia digital, la misma que es tendencia en diversos delitos donde se usan medios informáticos. En tal sentido, la aplicación de la medida de incautación de bienes informáticos no solo es de interés legal sino también como una importante fuente de practicidad en las investigaciones penales ante la evidencia digital.

CAPÍTULO IV

LA APLICABILIDAD DE LA MEDIDA PROCESAL DE INCAUTACIÓN DE BIENES AL DELITO *SIM SWAPPING*

4.1. Redefinición del alcance de los bienes sobre los que puede recaer la medida procesal de incautación de bienes

El desarrollo del tema expuesto a lo largo de la presente investigación indica que la medida procesal de incautación recae sobre bienes (muebles e inmuebles); sin embargo, se debe señalar que ante un hecho delictivo donde se usen herramientas informáticas, el trato para obtener evidencias es distinto a los delitos comunes, puesto que, el tipo penal vulnera el bien jurídico que es la seguridad de la información contenida en datos o sistemas informáticos.

En el caso del delito de *SIM swapping*, la conducta recae sobre bienes que están vinculados al IMEI y la información digital almacenada; sin embargo, al tratarse de un bien informático, no visible físicamente, el concepto se denota más amplio de lo previsto. En tal sentido, el dato informático es un concepto novedoso que no fue incluido en el tradicional concepto que maneja la legislación peruana y que ha sido incorporada por diferentes tratadistas; por ejemplo, para Arias de Rincón (2007), los datos informáticos son "segmentos de información numérica que circulan en la red, considerados como bienes muebles incorporales". Entendiéndose que la información es propiamente un bien, en el extremo que es susceptible de titularidad y, por ende, es necesario procurar su regulación en favor de la evolución del derecho y el desarrollo de la sociedad, por lo cual, se entiende que la medida de incautación fue diseñada de espaldas a la posible inclusión de los datos informáticos como bienes pasibles de ser incautados. No obstante, como se puede apreciar, no existe obstáculo conceptual ni de los principios del proceso, que impidan que el dato informático pueda ser objeto de esta medida de búsqueda de pruebas.

Estando al párrafo precedente, el grupo de investigación concluye que los ilícitos de carácter informático son delitos especiales, la propuesta interpretativa aquí defendida es que no podría excluirse la aplicación de la incautación a los delitos informáticos, especialmente en el delito de *SIM swapping*, debido a que, al tratarse de un delito realizado mediante medios tecnológicos, los datos informáticos son volátiles, es decir, son alterados o modificados con facilidad, por lo que, la aplicación de la medida procesal de la incautación garantizaría la ejecución exitosa de la medida procesal del levantamiento del secreto bancario, en el extremo que se obtendría acceso a los datos informáticos almacenados.

Ante el delito de *SIM swapping* como delito informático, los medios con los que cuenta el ordenamiento jurídico y los titulares de la acción penal, para obtener la información que permita identificar a los autores del delito, ya sea buscándola en el sistema bancario, en las bases de datos de las empresas de telecomunicación, toma un excesivo tiempo en obtenerse, lo que genera un riesgo en la información, siendo susceptible de que esta se pierda, pueda ser alterada o en el peor de los casos ser destruida por los mismos ciberdelincuentes.

Asimismo, la medida procesal de búsqueda de pruebas y restricción de derechos aplicable a este tipo de delitos es el levantamiento del secretario bancario, previsto en el artículo 235 del Código Procesal Penal; sin embargo, esta medida no es inmediata, ya que, al tratarse de documentación e información digital confidencial de los usuarios de servicios bancarios, con relación a los servicios que prestan las empresas del sistema, estas no pueden facilitar la información referente a las operaciones bancarias a terceros, salvo por mandato judicial; lo que demanda tiempo por parte del juez para otorgar esta autorización y así obtener la documentación requerida por las autoridades encargadas de la investigación del delito.

En tal sentido, ante esta problemática respecto a las limitaciones que presenta el levantamiento del secreto bancario, es posible recurrir a la aplicación de otras medidas

previstas en el Código Procesal Penal del 2004, en particular la medida procesal de Incautación de Bienes, en el sentido que esta medida va a recaer, sobre los datos informáticos que toda entidad bancaria resguarda sobre un usuario/cliente en particular.

Bajo esta premisa, entorno a la aplicabilidad de la medida procesal de incautación de bienes en el delito informático *SIM swapping*, es importante señalar que el principal objetivo de esta medida procesal es la aplicación de la misma sobre bienes o activos, en tal sentido, al ser una medida cautelar de naturaleza real, va recaer sobre objetos, instrumentos y demás *SIM*ilares; los mismos, que van a formar parte sustancial del delito (Ovalle, 2016). De esta manera se puede concluir en la idea de que no existe un impedimento normativo para proceder con la aplicación de dicha medida.

Resulta imperioso destacar los múltiples beneficios que la tecnología ha traído al desarrollo del hombre en sociedad, lo que genera un nuevo medio de interacción en un plano digital, donde ciertas actividades cotidianas resultan ser más factibles, sin embargo, y no siendo menos importante, este nuevo medio cibernético existente en el que se viene interactuando, permite la intervención de intrusos con fines delictivos en la web, lo que da como resultado la aparición de nuevas modalidades de delinquir a través de medios tecnológicos; dentro de ellos, la más inusual, por su *modus operandi*, es el denominado *SIM swapping* o suplantación de chip.

En tal sentido, la presente investigación, analiza las características del delito de *SIM swapping*, y si corresponde la aplicación de la medida de incautación de bienes (datos informáticos) para la investigación de tales ilícitos, ya que si bien es cierto los datos informáticos se encuentran en el móvil, este instrumento físico no incurre en importancia puesto que, si se plantea el escenario en el que la línea telefónica fue dado de baja por un tiempo determinado, tiempo en el cual el delincuente obtiene los datos informáticos contenidos en el mismo para posteriormente causar un perjuicio económico al titular

vaciando sus cuentas bancarias digitales. Además, la medida de incautación no va recaer sobre el equipo móvil como tal, sino en los datos informáticos contenidos en él, los cuales pueden ser rastreados por el IMEI, código que es extraído de la intervención a los datos de la cuenta bancaria en perjuicio y que son de administración de la entidad bancaria.

Si bien es cierto la normativa nacional no señala explícitamente la aplicación de esta medida procesal en delitos informáticos, empero nuestra posición tiene un respaldo internacional. Tal es el caso de Argentina en el que señala conforme al Código Procesal Penal Nacional en el artículo 151, la figura de la incautación de datos informáticos destacándose que el juez podrá ordenar el registro de un sistema informático o parte de este o un medio de almacenamiento informático con la finalidad de preservar u obtener una copia de los datos informáticos de interés para la investigación.

Por otro lado, se tiene la postura de la legislación chilena, la cual señala que la incautación de bienes informáticos requiere de un resguardo especial ya que existe cierta dificultad para delimitar el hallazgo exacto de las pruebas por el uso de un medio tecnológico, en este tipo de delitos la investigación será más minuciosa para la conservación y confiabilidad de las pruebas, teniéndose en cuenta que para dicho proceso se seguirá el mismo procedimiento de un delito común, y para su aplicación de esta medida el juez tiene que tener la certeza de que la evidencia presentada coincida con la prueba hallada, siendo así se aplicarán las cuatro etapas establecidas en el Código Procesal Penal de Chile (hallazgo de los hechos, inspección y búsqueda de indicios, fijación de la evidencia y recolección /embalaje de evidencias), para procesar y analizar la evidencia incautada.

En tal sentido, estando a que los ilícitos de carácter informático son delitos especiales, la propuesta interpretativa aquí defendida es que no podría excluirse la aplicación de la incautación a los delitos informáticos, especialmente en el delito de *SIM swapping*, debido a que, al tratarse de un delito realizado mediante medios tecnológicos, y los datos

informáticos son volátiles, es decir, son alterados o modificados con facilidad, esta medida limitativa permitiría obtener por medio del levantamiento del secreto bancario los datos que resguarda la entidad bancaria (cuenta bancaria) en la que están registrados todos los movimientos efectuados en la cuenta y por la cuenta, pudiéndose hallar el IMEI (equipo móvil-celular) y el IP (computadoras) y así poder rastrear la ubicación de quien sería el sujeto de la comisión de dicho tipo penal.

Aunado a ello, cabe señalar que la aplicación de la medida procesal de incautación sobre bienes informáticos como medida complementaria/alternativa al levantamiento del secreto bancario conlleva a una serie de ventajas, tales como los siguientes: búsqueda, retención, conservación y aseguramiento de los elementos que puedan servir como medios de prueba, impedimento a la obstaculización de la averiguación de la verdad y obtener las fuentes de prueba de forma inmediata que pueden servir como medios probatorios en etapa de juicio.

CONCLUSIONES

Primera. De acuerdo con el análisis desarrollado en esta investigación, se concluye que la medida limitativa de derechos *"levantamiento del secreto bancario"* no es la única figura procesal que permite resolver y reunir elementos de convicción que coadyuven al lograr un proceso eficaz con respecto al delito informático de *SIM swapping*, ya que, como se prevé en capítulos anteriores, la aplicabilidad de la incautación resulta ser una medida de rápida acción en comparación con la propuesta antecesora. Por consiguiente, este equipo de trabajo sostiene que mediante la aplicación de la incautación no solo se asegura una mayor celeridad del proceso que implica la investigación de este tipo de delitos informático, sino también existe una mayor eficiencia con respecto a los elementos de convicción recabados, en razón que existe una preservación de la prueba primogénita, la cual garantiza un juzgamiento veraz.

Segunda. Conforme al estudio del delito informático de *SIM swapping* a lo largo de la presente investigación se resalta que efectivamente el bien afectado es la información contenida en los datos y/o sistemas informáticos, por lo que, ante este tipo de escenario el titular de la acción penal a fin de poder recolectar evidencias que coadyuven al esclarecimiento de los hechos aplica la medida procesal del levantamiento del secretorio bancario; sin embargo, es evidente que no es la única medida para la investigación ya que conforme a nuestro estudio, la medida procesal de incautación de bienes en los delitos informáticos conforme a la base procesal penal es viable ya que el propósito de la misma es que no se manipulen, alteren o eliminen los datos informáticos los cuales son esencialmente parte para determinar el hecho ilícito.

Tercera. Respecto a la información recabada, se ha observado que el desarrollo del delito informático de *SIM swapping* nace en un escenario, en el que el proceso acelerado de la integración de la economía, la sociedad y la cultura (globalización) ha conllevado la

adopción de las tecnologías de información y comunicaciones (TIC) a la vida cotidiana del hombre. Por lo que, se obtiene como resultado consecuencias en cadena, la primera es la dependencia del ser humano con la tecnología, las leves limitaciones de administración de nuestros datos que como resultado exponen la fragilidad del respeto y protección a nuestra intimidad y privacidad, para finalmente en suma desatar una serie de alternativas y/o herramientas de fácil acceso empleadas con fines delictivos y en perjuicio de esta sociedad denominada "sociedad de la información".

Cuarto. La aplicación de la interpretación analógica en la presente investigación se justifica en la naturaleza de la misma, al ser un fundamento del derecho, siendo que el supuesto presentado para su aplicación no implica un perjuicio para el imputado, es decir, la presente tesis no plantea una analogía *in malam partem*, tampoco busca y/o genera un beneficio hacia el imputado. En consecuencia, no se puede exceptuar la primicia con la que con la que se inició este argumento; en el extremo que, no es pertinente la limitación de este mecanismo a lo que la norma adjetiva prevé, más aún cuando el presupuesto no pretende contravenir a lo establecido, sino que busca integrar la norma a un caso en concreto, cuyo fin es contribuir con el proceso y velar por la preservación de la prueba, a fin de lograr resarcir en la medida de lo posible el perjuicio generado a la víctima.

REFERENCIAS

Acuerdo Plenario N.° 5-2010/CJ- 116 (16-11-2010). Mediante el VI Pleno Jurisdiccional de las Salas Penales Permanente y Transitoria.

Arias de Rincón, M. (2007). La calificación jurídica de las trasmisiones de software en Internet, *Frónesis*, *14*(1).

Bramont-Arias, L. (1997). *El delito informático en el Código Penal Peruano,* Biblioteca de Derecho Contemporáneo, Fondo Editorial.

Cáceres, R. (2008). *El proceso de pérdida de dominio y las medidas cautelares en la investigación preliminar*. Editorial IDEMSA.

Castillo, M. & Ramallo, M. (1989). El delito informático. Facultad de Derecho de Zaragoza. *Congreso sobre Derecho Informático*. 22-24.

Chen, S. (2010). Privacidad y Protección de datos: Un análisis de Legislación Comparada. Diálogos *Revista Electrónica de Historia. 11*(1), 111-152.

Código Penal Español (24-05-1996). Delitos Informáticos. Ley Orgánica 1/2015, que modifica la Ley Orgánica 10/1995.

Código Procesal Constitucional (31-05-2004). Ley N.° 28237. Normas Legales actualizadas, El Peruano.

Código Procesal Penal (29-07-2004). Código Procesal Penal. Séptima Edición Oficial (www.gob.pe)

Conacop (2020). *Diagnóstico multisectorial sobre la ciberdelincuencia en el Perú. Ministerio de Justicia y Derechos Humanos.* Primera Edición digital.

Constitución de Chile de la República de Chile (1980).

Constitución de la República Bolivariana de Venezuela (1999). *Gaceta Oficial Extraordinaria N.° 36.860.*

Convenio sobre la Ciberdelincuencia (23-11-2001*).* Budapest, Serie de Tratados Europeos-N.° 185.

Consejo de Europa-División de Ciberdelito (2021). *Convenio de Budapest sobre la Ciberdelincuencia.* Consejo de Europa.

Contreras, R. (16/11/2020). El fenómeno delictual informático del *SIM* swapping o suplantación de la tarjeta *SIM*. *Enestrado-Actualidad jurídica minuto a minuto.*

Decreto Supremo N.°10-2019-RE (01-12-2019). Ratifican el Convenio sobre la Ciberdelincuencia.

Diario El Peruano (2023). ¡Cuidado con los fraudes informáticos! Estas son las modalidades más denunciadas en Perú. Editora Perú.

Hermosillo, M. (2021). *El principio de mismidad.* Frontera.

Hugo, S. (2014). *Tipificación de los delitos informáticos patrimoniales en la Nueva Ley de Delitos Informáticos N.° 30096*. Alma máter Segunda Época.

INEI (2023). *Estadísticas de la criminalidad, seguridad ciudadana y violencia.* Informe Técnico N.° 02-junio 2023.

Landa, C. (2017). *Los derechos fundamentales.* Colección lo Esencial del Derecho N.º 2. Fondo Editorial PUCP.

Ley de Enjuiciamiento Criminal (14-09-1882).

Ley Especial contra Delitos Informáticos (30-10-2001). Gaceta Oficial de la República Bolivariana de Venezuela. *Gaceta Oficial N.º 37313*.

Ley N.° 5020 (22-12- 2014). La legislatura de la provincia de Río Negro.

Ley N.° 10. (26-06-2014). Ley de Ordenación, Supervisión y Solvencia de Entidades de Crédito. Ley N.° 10.

Ley N.° 1273 (05-01-2009). Ley de Delitos Informáticos en Colombia. Congreso de la República de Colombia.

Ley N.° 21526 (14-02-1977). Ley de Entidades Financieras de Buenos Aires.

Ley N.° 21.459 (20-06-2022). Ley que establece normas sobre delitos informáticos y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. Ley Chile. Ley 21459-Biblioteca del Congreso Nacional (bcn.cl).

Ley N.° 26388 (24-06-2008). Ley de Delitos Informáticos Congreso de la Nación de Argentina.

Ley N.º 29733. (03-07-2011). Ley de Protección de Datos Personales. Reglamento de la Ley N.º 29733 mediante el Decreto Legislativo 1353. Normas legales actualizadas. Diario El Peruano.

Ley N.° 30096 (21-10-2013). Ley de Delitos Informáticos y su modificatoria Ley N.° 30171 Norma legal. *Diario Oficial El Peruano*.

Ley N ° 30171 (17-02-2014). Ley de Delitos Informáticos. Norma legal. *Diario Oficial El Peruano*

Ley N.° 31507 (03-07-2022). Ley de Reforma Constitucional que fortalece la lucha anticorrupción en el marco del Levantamiento del Secreto Bancario y la Reserva Tributaria.

Ley N.° 906 (31-08-2004). Código de Procedimiento Penal de Colombia.

Ministerio de Relaciones Exteriores. (2017). *Derecho Penal Informático*. Segunda Edición.

Ministerio de Transportes y Comunicaciones (2022). Cómo evitar ser víctima de fraude digital mediante la duplicación del chip de tu teléfono móvil. *Plataforma digital del MTC.*

Ministerio del Interior (2020). *Manual de recojo de evidencia digital. P.* Primera Edición Ministerio del Interior 2020.

Ministerio Justicia y Derechos Humanos (2017). *Manual de Evidencia Digital.* Primera edición, julio 2017.

Ministerio Público (2020). *Guía de Análisis Digital Forense del Ministerio Público.* Goperit/Gui-01. (documento interno del MP, primera guía)

Montesquieu (1906). *El espíritu de las Leyes, Tomo I.* Librería General de Victoriano Suárez. Editorial Tecnos.

Naked Security (2020). Desarticulan en España una organización criminal internacional especializada en *SIM* swapping. *Sophos News.*

Ovalle, J. (2016). *Teoría general de la prueba. Curso teoría general del proceso.* Oxford.

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

Priori, G. (2003). La efectiva tutela jurisdiccional de las situaciones jurídicas materiales: hacia una necesaria reivindicación de los fines del proceso. *Revista Ius et Veritas, 26,* 279-280.

Recurso de Casación 864-2017/Nacional (21-05-2018). *Corte suprema de justicia de la república, sala penal permanente-ponente: César San Martín Castro.*

Resolución N.° 1477-2022/SPC-Indecopi (21-07-2022). Exp. N.° 0064-2020/CPC-Indecopi-CHT, Sala Especializada en Protección al Consumidor del Tribunal de Defensa de la Competencia y de la Propiedad Intelectual.

Resolución N.° 1208-2022/SPC-Indecopi (16-06-2022). Emitida Sala Especializada en Protección al Consumidor del Tribunal de Defensa de la Competencia y de la Propiedad Intelectual.

Resolución Legislativa N.° 30913 (13-02-2019. Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia - Resolución Legislativa N.° 30913. Congreso de la República. Diario Oficial El Peruano.

Resolución N.° 32 (08-07-2019). Exp. 00228-2016-1-5001-JR-PE-04. Primera Sala Penal de Apelaciones Nacional Permanente Especializada en Crimen-Organizado-(Torre-Muñoz).

Resolución N.° 072-2022-CD/OSIPTEL. (07-04-2022). N.° 072-2022-CD/OSIPTEL

Resolución Administrativa N.º 387-2014-CE-PJ (23/04/2014). Protocolo de actuación conjunta referido al allanamiento. Poder Judicial.

Ramos, C. (2011). *Cómo hacer una tesis de derecho y no envejecer en el intento*. Editorial y Librería Jurídica Grijley. Iustitia.

Rodríguez, B. (2006). *Metodología jurídica. Colección Textos Jurídicos Universitarios.* Editorial Oxford University Press.

Rodríguez, F. (2013). *Derecho informático. El derecho en la era digital. La sociedad de información y el sistema jurídico. Contratos Informáticos. Protección jurídica de los programas de computación. Delitos informáticos. La tutela jurídica del sistema informático.* Editorial UNC.

San Martín, C. (2020). *Derecho procesal penal lecciones (2da ed.).* INPECCP-CENALES

Santelices, V. (2014). Tratamiento de la evidencia contenida en soportes informáticos como prueba en el proceso penal. *Actualidad Jurídica*. *29*(15), 545-548.

Senado y la Cámara de Diputados de la Nación Argentina. (04-09-1991). Código Procesal Penal de la Nación de Argentina.

Sentencia Tribunal Constitucional Exp. N.° 0751-2002-AA-TC (04-11-2002). Exp. N.° 0751-2002-AA-TC.

Sentencia Tribunal Constitucional Exp. N.° N.° 763-2005-PA/TC (13-04-2005). Exp. N.° N.° 763-2005-PA/TC.

Sentencia Tribunal Constitucional Exp. N.º 04739-2007-PHD/TC (15-10-2007). Exp. N.º 04739-2007-PHD/TC (fundamento 2-3).

Téllez, J. (1998). Delitos cibernéticos. *informática y derecho: Revista Iberoamericana de Derecho Informático (segunda época*). 27-29, 113-116.

Vergara, A. (1990). *El secreto bancario sobre su fundamento, legislación y jurisprudencia*. Editorial Jurídica de Chile.

Villavicencio, F. (2014). Delitos informáticos. *Ius Et Veritas*, 49, 288-289.

Villazán, J. (2009). *Manual de Informática I.* Universidad Michoacana de San Nicolás de Hidalgo.

Witker, J. (1986). *Cómo elaborar una tesis en derecho. Pautas metodológicas y técnicas para el estudiante o investigador del derecho.* Civitas.

Zambrano, A. (2022). El levantamiento del secreto bancario aplicado al delito informático *SIM swapping / entrevistado por Sarela Málaga*. Arequipa.