Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

EL CIBERCRIMEN EN EL PERÚ: ASPECTOS SUSTANTIVOS Y PROCESALES

Línea de investigación:
Gobernabilidad, derechos humanos e inclusión social

Tesis para optar el Grado Académico de Doctor en Derecho

Autor

Mori Quiroz, Francisco

Asesora

Borjas Guerra de Alarcón, Mirtha Janet

ORCID: 0000-0003-3192-7717

Jurado

Aramayo Cordero, Uriel Alfonso

López Navarro, Lindbergh

Morante León, Salomón Jorge

Lima - Perú

2025

Document Information

Analyzed document	1A_MORI_QUIROZ_FRANCISCO_DOCTORADO_2023.docx (D169906406)
Submitted	2023-06-06 22:33:00 UTC+02:00
Submitted by	Johnny
Submitter email	jastete@unfv.edu.pe
Similarity	25%
Analysis address	jastete.unfv@analysis.urkund.com

Sources included in the report

SA	**Universidad Nacional Federico Villarreal / 1A_Mori_Quiroz_Francisco_Maestria_2017.pdf** Document 1A_Mori_Quiroz_Francisco_Maestria_2017.pdf (D30016480) Submitted by: fcaldas@unfv.edu.pe Receiver: fcaldas.unfv@analysis.urkund.com	46
SA	**Universidad Nacional Federico Villarreal / 1A_ACOSTA_HERNANDEZ_HERMEL_MAESTRIA_2019.docx** Document 1A_ACOSTA_HERNANDEZ_HERMEL_MAESTRIA_2019.docx (D59273329) Submitted by: repositorio.vrin@unfv.edu.pe Receiver: repositorio.vrin.unfv@analysis.urkund.com	3
SA	**Universidad Nacional Federico Villarreal / 2A_ Mori_Quiroz_Francisco_Maestria_2017_docx..doc** Document 2A_ Mori_Quiroz_Francisco_Maestria_2017_docx..doc (D31929783) Submitted by: fcaldas@unfv.edu.pe Receiver: fcaldas.unfv@analysis.urkund.com	30
SA	**Universidad Nacional Federico Villarreal / 1A_LECAROS_SABOYA_ERIKA_MANUELA_MAESTRIA_2022.docx** Document 1A_LECAROS_SABOYA_ERIKA_MANUELA_MAESTRIA_2022.docx (D142453993) Submitted by: jastete@unfv.edu.pe Receiver: jastete.unfv@analysis.urkund.com	1
W	URL: https://repository.ucc.edu.co/bitstream/20.500.12494/19788/3/2020_analisis_delitos_informaticos.pdf Fetched: 2021-06-28 03:00:25	1
W	URL: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf Fetched: 2019-09-28 18:48:45	10
W	URL: http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf Fetched: 2020-11-15 09:06:52	5
SA	**e89f7a02f3d809036dc49ccae65fb63b4fc393d3.html** Document e89f7a02f3d809036dc49ccae65fb63b4fc393d3.html (D166490439)	1

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

EL CIBERCRIMEN EN EL PERÚ: ASPECTOS SUSTANTIVOS Y PROCESALES

Línea de Investigación:

Gobernabilidad, Derechos Humanos e Inclusión social

Tesis para optar el Grado Académico de

Doctor en Derecho

Autor

Mori Quiroz, Francisco

Asesor

Borjas Guerra de Alarcón, Mirtha Janet

ORCID: 0000-0003-3192-7717

Jurado

Aramayo Cordero, Uriel Alfonso

López Navarro, Lindbergh

Morante León, Salomón Jorge

Lima- Perú

2025

DEDICATORIA

A Dios por concederme la sabiduría, a mis padres, esposa e hija quien por ellos soy lo que soy, por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles. Me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para conseguir mis objetivos.

AGRADECIMIENTO

A la Escuela de Postgrado de la Universidad Nacional Federico Villarreal, por brindarme la oportunidad de realizar los estudios de Doctorado, a mis compañeros de estudios por estar en todo momento en clases recibiendo los conocimientos, a mis profesores de maestría que me dieron sus conocimientos para culminar mis estudios de Doctorado, y a los jurados examinadores de la tesis. Con sincera gratitud a las personas que contribuyeron y brindaron valiosos aportes, críticas, constructivas, apoyo moral y material para la materialización de la tesis.

ÍNDICE

RESUMEN viii

ABSTRACT ix

RIASSUNTO x

I. INTRODUCCIÓN 11

1.1. Planteamiento del problema 16

1.2. Descripción del problema 18

1.3. Formulación del problema 23

1.3.1. Problema general *23*

1.3.2. Problemas específicos *23*

1.4. Antecedentes de la investigación 23

1.4.1. Antecedentes nacionales *23*

1.4.2. Antecedentes internacionales *29*

1.5. Justificación de la investigación 38

1.5.1. Justificación práctica *39*

1.5.2. Justificación Doctrinaria – Dogmática *42*

1.5.3. Justificación jurídica *43*

1.6. Limitaciones de la investigación 45

1.7. Objetivos 45

1.7.1. Objetivo general *45*

1.7.2. Objetivos específicos *45*

1.8. Hipótesis 46

1.8.1. Hipótesis general *46*

1.8.2. Hipótesis específicas *46*

II. MARCO TEÓRICO 47

2.1. Marco conceptual 47
2.2. Bases teóricas 53
2.3. Marco histórico 121
2.4. Marco filosófico 124
2.5. Bases Legales 127
III. MÉTODO 132
3.1. Tipo de investigación 132
3.2. Población y muestra 134
3.3. Operacionalización de variables 138
3.4. Instrumentos 145
3.5. Procedimientos 145
3.6. Análisis de datos 146
IV. RESULTADOS 147
V. DISCUSIÓN DE RESULTADOS 165
VI. CONCLUSIONES 173
VII. RECOMENDACIONES 174
VIII. REFERENCIAS 176
IX. ANEXOS 184
Anexo A. Matriz de consistencia 184
Anexo B. Encuestas 185
Anexo C. Validación y confiabilidad de instrumentos 189

ÍNDICE DE TABLAS

Tabla 1 Muestra de estudio 136

Tabla 2 Operacionalización de variables 138

Tabla 3 Vacíos Jurídicos – Penales 147

Tabla 4 Ausencia de Formación Tecnológica en Delitos Informáticos. 148

Tabla 5 Transgresiones de las Legislaciones Vigentes 149

Tabla 6 Insuficiencia Jurisprudencial 150

Tabla 7 Valoración impropia determinación del tipo penal 152

Tabla 8 Inadecuada determinación del daño causado 153

Tabla 9 Insuficiente cálculo del monto indemnizatorio 154

Tabla 10 Incidencia delictiva / informática 155

Tabla 11 Niveles de frecuencia de la variable independiente 157

Tabla 12 Tabla de frecuencia de la Dimensión I 157

Tabla 13 Tabla de frecuencia de la Dimensión 2 159

Tabla 14 Prueba de normalidad de las variables 160

Tabla 15 Prueba Rho de Spearman de la dimensión 161

Tabla 16 Prueba de normalidad de la dimensión 2 163

Tabla 17 Estadístico de fiabilidad, Alpha de Cronbach del instrumento 189

ÍNDICE DE FIGURAS

Figura 1 Muestra de estudio.....136

Figura 2 Niveles de consenso entre Operadores de Justicia 148

Figura 3 Niveles de ausencia de Formación Tca. 149

Figura 4 Niveles de consenso entre Operadores de Justicia sobre el marco teórico 150

Figura 5 Consenso de los Operadores de Justicia para solucionar vacíos legales en Delitos Informáticos 151

Figura 6 Consenso entre Operadores de Justicia para combatir la determinación del tipo penal 152

Figura 7 Consenso de los Operadores de Justicia sobre determinación del daño causado…153

Figura 8 Consenso del (89%) de los Operadores de Justicia sobre insuficiente monto indemnizatorio 154

Figura 9 Consenso del (75.7%) para prevenir y evitar los Delitos Informáticos.....156

Figura 10 Niveles de frecuencia de la dimensión 1: Limitaciones en torno a la aplicabilidad de los aspectos sustantivos – penales.....158

Figura 11 Niveles de frecuencia de la dimensión 2 159

Figura 12 Dispersión de las variables 162

RESUMEN

En el desarrollo de la presente investigación se ha tratado acerca de "El Cibercrimen en el Perú, y sus Aspectos Sustantivos como Procesales, en el Distrito Judicial de Lima, durante el periodo 2017 – 2018", en que se ha tenido por objetivo central en poderse determinar sobre la relación de influencia que llegan a tener los problemas de falta de aplicabilidad de los aspectos sustantivos/penales como procesales sobre los procesos penales – judiciales respecto a imputados por ilícitos informáticos, y de cómo ha venido repercutiendo sobre la incidencia y erradicación de los delitos de cibercrimen perpetrados mayormente en la ciudad de Lima Metropolitana, entre los años indicados; lo que se ha podido desarrollar de conformidad a un estudio metodológico de tipo básico y de nivel descriptivo con diseño correlacional sobre una muestra de 82 operadores jurídicos entre Fiscales y Jueces Penales que ejercen en Lima y que fueron encuestados con un cuestionario de 24 ítems, de cuyas respuestas que se analizaron de manera contrastable para la respectiva validación de las hipótesis formuladas, se validó con un coeficiente Spearman principal de 0.873, que valida la problemática planteada en torno a la hipótesis principal de estudio; y con un promedio del 55% de los operadores encuestados que señalaron acerca de la problemática existente de la falta de aplicación de los criterios sustantivos como procesales más eficaces al respecto, a causa de desconocimientos por parte de los propios operadores sobre qué criterios deben ejecutar en sí, para hacer más eficaces los litigios judiciales respectivos y de resolverlos de manera contundente; lo que sumándose a las situaciones complejas de que los delincuentes informáticos tienden a eliminar las pruebas informáticas existentes; llega a implicar finalmente que los casos bajo litigio judicial al respecto, no se resuelvan con la efectividad contundente requerida.

Palabras clave. Aspectos, delitos informáticos, Operadores jurídicos, Procesales y Sustantivos.

ABSTRACT

In the development of this research has been about "Cybercrime in Peru, and its Substantive Aspects as Procedural, in the Judicial District of Lima, during the period 2017 - 2018", in which the main objective has been in be able to determine the influence relationship that problems of lack of applicability of substantive / criminal as well as procedural aspects have on criminal-judicial processes regarding those accused of computer illicit crimes, and how it has been having an impact on the incidence and eradication of cybercrime crimes perpetrated mainly in the city of Metropolitan Lima, between the years indicated; what has been possible to develop in accordance with a methodological study of a basic type and descriptive level with correlational design on a sample of 82 legal operators among prosecutors and criminal judges who practice in Lima and who were surveyed with a questionnaire of 24 items, of The responses of which were analyzed in a testable way for the respective validation of the formulated hypotheses, was validated with a main spearman coefficient of 0.873, which validates the problems raised around the main hypothesis of the study; and with an average of 55% of the operators surveyed who indicated about the existing problem of the lack of application of the substantive criteria as more efficient procedural in this regard, due to ignorance on the part of the operators themselves about which criteria they should execute in Yes, to make the respective legal disputes more effective and to resolve them forcefully; What adding to the complex situations that cybercriminals tend to eliminate existing computer evidence; it finally implies that the cases under judicial litigation in this regard are not resolved with the forceful effectiveness required.

Keywords. Aspects, computer crimes, legal operators, procedural and substantive.

RIASSUNTO

Questa ricerca ha affrontato il tema "La criminalità informatica in Perù e i suoi aspetti sostanziali e procedurali nel distretto giudiziario di Lima, nel periodo 2017-2018". L'obiettivo principale era determinare l'influenza che i problemi di inapplicabilità degli aspetti sostanziali/penali e procedurali hanno sui procedimenti penali-giudiziari contro gli accusati di reati informatici e come ciò abbia influito sull'incidenza e l'eradicazione dei reati informatici, perpetrati principalmente nell'area metropolitana di Lima negli anni indicati. che è stato sviluppato in conformità con uno studio metodologico di base e un livello descrittivo con disegno correlazionale su un campione di 82 operatori legali tra Pubblici Ministeri e Giudici Penali che esercitano a Lima e che sono stati intervistati con un questionario di 24 domande, le cui risposte, analizzate in modo verificabile per la rispettiva convalida delle ipotesi formulate, sono state convalidate con un coefficiente di Spearman principale di 0,873, che convalida il problema posto attorno all'ipotesi principale dello studio; e con una media del 55% degli operatori intervistati che ha segnalato il problema esistente della mancata applicazione di criteri sostanziali come la procedura più efficace a tale riguardo, a causa dell'ignoranza da parte degli operatori stessi su quali criteri dovrebbero eseguire al fine di rendere le rispettive controversie giudiziarie più efficaci e risolverle in modo definitivo; ciò si aggiunge alle complesse situazioni in cui i criminali informatici tendono a eliminare le prove informatiche esistenti; ciò significa in definitiva che i casi oggetto di contenzioso giudiziario non vengono risolti con l'efficacia richiesta.

Parole chiave. Aspetti, criminalità informatica, operatori giuridici, procedurali e sostanziali.

I. INTRODUCCIÓN

Este estudio aborda la problemática de la ciberdelincuencia y/o el cibercrimen en el Perú, con un análisis centrado en los aspectos sustantivos y procesales que inciden en su tratamiento penal dentro del Distrito Judicial de Lima, durante el periodo 2017 - 2018. Que consta de un conjunto de acciones ilícitas que se ejecutan utilizándose los medios electrónicos – informatizados y de manera cada vez más sistematizada, planificada y organizada, que pueden llegar a atentar gravemente contra los bienes jurídicos esenciales de la información y sistemas informáticos de las organizaciones empresariales privadas, de Entidades Públicas Estatales, y de las personas naturales que disponen de sus datos personales en medios, programas o instrumentos informáticos, que son transgredidos, interceptados y vulnerados por delincuentes informáticos o hackers que acceden u obtienen ilegalmente información que no les concierne, y cometen a su vez delitos graves en contra del patrimonio económico de las organizaciones vulneradas, y contra el honor reputacional de las personas afectadas; llega así a tenerse que los crímenes perpetrados por los ciberdelincuentes son cada vez más frecuentes y más peligrosos con resultados dañinos y colaterales negativos, no solamente para las personas jurídicas y naturales agraviadas, también tienen impacto en el orden socio - económico, financiero y hasta de grave afectación para la misma seguridad pública del Estado Peruano.

En este aspecto destaca la importancia del estudio por las investigaciones que se han realizado para conocer las violaciones informáticas o la seguridad penal de los bienes jurídicos que han sido quebrantados con tales infracciones, lo que incluye el legado económico de los seres humanos, la confidencialidad de la información secreta, e incluso la proximidad y la intimidad personal respecto a los ciudadanos cuya privacidad es violada a través de este aspecto. El impacto científico es ayudar a encontrar soluciones a problemas acuciantes a la luz de los avances de la tecnología, se desarrolló en este estudio un instrumento científico tecnológico que sea útil a los operadores de justicia (jueces, fiscales y las fuerzas del orden)

del Distrito Judicial de Lima dedicados a la investigación y acusación de delitos informáticos y a la salvaguarda penal de la confianza.

En materia sustantiva, Abdulai (2016) muestra una correlación entre los patrones de uso de Internet de los estudiantes y su nivel de preocupación y peligro de ser objeto de estafas con tarjetas de crédito/débito. Sin embargo, la ansiedad y el peligro de los estudiantes, así como su experiencia de explotación y sus hábitos de uso de Internet, no fueron predichos de forma significativa por sus características sociodemográficas o su conocimiento de la ciberdelincuencia.

Por su parte, Wan (2016) señala que China cuenta con una estructura normativa de varios niveles en relación con los actos cibernéticos malintencionados, que incluye los instrumentos fundamentales y primarios, así como las dos enmiendas. Aunque ambas enmiendas han ampliado la definición de ciberdelincuencia, sus motivaciones para hacerlo varían. Para abordar el vacío generado por el incremento en la popularidad de los ordenadores personales, se publicó la Enmienda (VII) en 2009. Este cambio solidificó la estrategia unidimensional de dos puntos. Este método distingue claramente entre los delitos cometidos con el uso de un ordenador y los cometidos utilizando un ordenador para cometer otros tipos de delitos (es decir, delitos contra la integridad de la información almacenada en el sistema informático y los datos.

Alanezi (2015) investigó las medidas adoptadas por las instituciones financieras saudíes para prevenir el fraude en línea y el efecto que estas medidas tenían tanto individual como colectivamente. Advierte de que, a medida que cada vez más actividades como socializar, comprar y realizar operaciones bancarias se trasladan a ordenadores y dispositivos móviles, aumenta el riesgo de ser pirateado o víctima de estafadores

Gonzáles (2013), jurista español, en su estudio está ampliando las sanciones penales para los ciberdelitos. Sin embargo, parece justo comenzar con una breve, pero vital orientación

hacia la ciencia de la que derivan los comportamientos posteriormente estudiados. Es bien sabido que la legislación, que sirve como aspecto regulador de las interacciones sociales, no puede predecir completamente los cursos que éstas toman a medida que evolucionan según las diferentes teorías. Este razonamiento se aplica igualmente a la situación asociada a los delitos informáticos en sentido amplio, que podemos denominar aquellos perpetrados contra, o a través de, medios informáticos. Este problema se ha visto agravado por el rápido desarrollo de las tecnologías asociadas a la información y la comunicación.

En el contexto peruano, Pardo (2018) analizó cómo el ordenamiento jurídico trata los delitos digitales contra el patrimonio en el Circuito Regional de Lima en el año 2018. Se llevó a cabo una serie de entrevistas con expertos en el área, tanto a nivel nacional como internacional, utilizando una guía de entrevistas para recolectar información que permitiera llegar a conclusiones sólidas sobre el tema. Se constató que la inclusión poco coherente de diversas formas de delitos electrónicos contra el patrimonio en la definición de fraude informático hace que el enfoque del derecho penal respecto a los delitos patrimoniales sea inapropiado. Esta ambigüedad normativa dificulta la imposición de sanciones efectivas para tales actos delictivos.

Sequeiros (2016) sostiene que, en los últimos años ha surgido un nuevo tipo de delitos conocidos como delitos informáticos, como consecuencia directa de los avances en la tecnología informática. En el Perú se han promulgado leyes para hacer frente a esta tendencia delictiva emergente, con el objetivo de prevenir y sancionar las actividades delictivas que involucran computadoras, datos informáticos, información privada de conversación, así como bienes jurídicos como el patrimonio, la fe pública y la libertad sexual. La "Ley de Delitos Informáticos" (Ley N° 30096) fue promulgada el 21 de octubre de 2013 y publicada oficialmente en "El Peruano" al día siguiente (22 de octubre de 2013). Posteriormente, los días

9 y 10 de marzo de 2014, se publicó la "Ley que actualiza la Ley 30096, Ley de Delitos Informáticos en Internet" (Ley Nº 30171), la cual fue aprobada para realizar ciertos cambios.

Sánchez (2017), sostiene que, la adopción de técnicas de ciberseguridad afecta significativamente a la seguridad de la información almacenada en la Oficina Económica del Pentágono, y señala, entre otras cosas, que ésta carece de medidas de protección contrarias y que su aplicación, así como los artilugios a su servicio, no son punteros.

Fernández et al. (2010) como resultado de su investigación, extraen dos conclusiones: en primer lugar, que, a diferencia de los avances tecnológicos, existe una mayor cantidad de propuestas de desarrollo en el delincuente, dado que éste ha obtenido un amplio conocimiento sobre estas Mejoras y que no las incluye en el do-gooding; y en segundo lugar, que el modo de vida ha cambiado tan drásticamente en los últimos 20 años que nos enfrentamos a nuevos tipos ilegales. Debido a que nuestro Poder Judicial, en particular la Ley 27309, dada el 26 de junio de 2000, emplea la categoría de "Delitos Informáticos" al Código Procesal Penal, en sus artículos 207-A, los delitos informáticos representan un vacío importante en nuestras leyes penales.

Al considerar la multitud de datos presentes en el ámbito digital, podemos crear una lista que incluye delitos que no están previstos en nuestro marco legal y que requieren ser examinados por académicos, criminalistas y legisladores. Empeoramiento de las condiciones de las piezas anteriores. La ley tiene que ponerse al día con la tecnología, que ahora se traduce en una tipificación inadecuada y en el uso de un lenguaje muy especializado y difícil de entender. La única estrategia de seguridad infalible emplea varios niveles de protección, pero es esencial establecer primero que ningún instrumento de control puede satisfacer todas las necesidades posibles.

La principal salvaguarda para no convertirse en víctima de la ciberdelincuencia, los cortafuegos, son ineficaces contra diversas formas de violaciones de la seguridad, incluidas las

internas, las físicas y las invasiones inducidas por la exposición de las contraseñas de los usuarios. La Policía Nacional del Perú, como lo demuestra la DIVINDAT, tiene la responsabilidad de hacer frente a los delitos informáticos y adoptar nuevos controles, evaluaciones de riesgos y medidas de seguridad para disminuir el impacto de la ciberdelincuencia.

Por otro lado, la investigación se justificó de forma doctrinaria-dogmática, se espera que este estudio sobre los delitos informáticos, habida cuenta de que, tras una década de vigencia de tales delitos tipificados en la Ley N° 30096 del 2013 y acorde con su última modificatoria basado en la Ley N° 30171 del 2014; se necesita esencialmente de una fundamentación doctrinaria penal exhaustiva y rigurosamente sustentable sobre la interpretación de dichos ilícitos acorde a lo tipificado en la Normatividad Penal, a efectos de poderse sustentar los aspectos sustantivos de tales ilícitos, de manera completa, exhaustiva y sin problemas de vacíos legales; y que asimismo contándose con los fundamentos dogmáticos y casuísticos - prácticos necesarios se pueda facilitar a los operadores jurídicos – procesales (Fiscales y Jueces Penales) de que puedan llegar a contar con toda la fundamentación requerida para que puedan sustentar los alegatos con que deban fundamentar las denuncias penales que deben interponerse contra autores por comisión de delitos informáticos, y asimismo para fundamentarse las órdenes o mandatos fiscales de prisión preventiva y de otras medidas coercitivas sobre imputados por grave comisión de dos o más ilícitos informáticos en forma de crimen organizado.

Por lo anteriormente mencionado, el presente trabajo tuvo como objetivos, explicar las limitaciones que se presentan en torno al tratamiento aplicable de los aspectos sustantivos – penales de los delitos informáticos, y cómo influyen sobre la penalización y disminución del cibercrimen y explicar los problemas que se presentan en torno al desarrollo de los aspectos procesales – penales sobre delitos informáticos, y cómo influyen sobre la penalización y

disminución del cibercrimen en el Distrito Judicial de Lima, durante los años 2017 – 2018 en el Distrito Judicial de Lima.

Respecto a informática y derecho penal, Maurach citado por Hurtado (1987) sostiene que no se trata sino de una exigencia ética planteada al legislador. De ahí que el Derecho penal sólo debe intervenir en aquellos actos que atenten gravemente contra bienes jurídicos protegidos. “Su intervención debe ser útil; de lo contrario pierde su justificación” (p. 28)

Respecto a delito informático, Téllez (1996) señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)" (p. 2).

1.1. Planteamiento del problema

A nivel global, se puede precisar que si bien en los países anglosajones como los Estados Unidos de Norteamérica, Inglaterra y Canadá, y en los países potencias europeas como Alemania y Francia, llegan a disponer de una legislación penal – sustantiva amplia que contempla todas las modalidades ilícitas referentes a los delitos informáticos, además de poder incluir dentro de la categoría punitiva de tales delitos, a nuevos ilícitos informáticos relacionados al ciberterrorismo, y que inclusive a nivel procesal, los sistemas judiciales de tales países llegan a disponer de los mecanismos jurídicos – procesales necesarios para un efectivo y hasta inmediato procesamiento judicial de los imputados por tales delitos.

Pero aun así, se tienen los problemas de afectación de garantías procesales para los delincuentes informáticos que son imputados y procesados al respecto, dado que son tratados bajo la condición de cibercriminales o de terroristas cibernéticos con alto prontuario ilícito, que se les llegan a imponer penas excesivamente drásticas, sin realizárseles una adecuada imputación penal en función acorde con la gravedad del delito informático que hayan perpetrado, y si han actuado por primera vez o en forma reincidente.

Actualmente puede comprobarse como el empleo de computadoras de todo tipo, marca, modelo y tamaño, esto es la informatización, tanto en la organización y administración de empresas, sean públicas y privadas dedicadas a la investigación periodística, técnica y científica e incluso en el ocio, el entretenimiento, posibilita que la informática sea indispensable y hasta conveniente sin embargo podrían ser utilizados por manos inescrupulosas para cometer diferentes Delitos Informáticos, circunstancia que no es más que consecuencia del continuo y progresivo desarrollo del campo de la informática, aplicada en la actualidad a todos los aspectos de la vida cotidiana.

Ya en otros países latinoamericanos como en México y Colombia, han podido ampliar la tipificación punitiva de los delitos informáticos según su legislación penal – sustantiva correspondiente; pero todavía se mantienen los problemas de discordancias y confusiones, entre ilícitos informáticos que vulneran diversos bienes jurídicos protegidos como también intereses difusos; y de que asimismo todavía no han llegado a desglosar con mayor precisión la clasificación de delitos informáticos por nivel de gravedad, si se tratan de meros ilícitos comunes o de si se han perpetrado en modo de crimen organizado, e incluso de soslayarse las conductas típicas - ilícitas de modalidades delincuenciales - informáticas vinculadas al ciberterrorismo; mientras que nivel de aspectos procesales, aún los operadores jurídicos - penales como Jueces y Fiscales Penales en tales países, poseen ciertas carencias en aplicar criterios procesales más rápidos y efectivos para procesar y condenar a los imputados delictivos / hackers informáticos, dada la acérrima capacidad prontuariada y peligrosa de tales sujetos criminales de borrar o desaparecer las pruebas informáticas que les impliquen, y con ello así poder consumar que se dilaten sus procesos penales - judiciales, como de que también escaseen los medios probatorios contundentes; para poder así obtener finalmente penas muy benignas o irrisorias, o hasta asimismo lograr la absolución judicial, o incluso de salir absueltos antes de

iniciarse el juicio oral, es decir durante la etapa de investigación procesal o en torno a la subfase de pre-instrucción penal correspondiente.

1.2. Descripción del problema

En el Perú, se tiene también en cierta forma los problemas señalados anteriormente, en que primeramente, la Ley Penal contra delitos informáticos, es decir la Ley N° 30096 de fecha 22 de octubre de 2013, llega a establecer penas benignas para determinados ilícitos informáticos, y que a su vez también se tienen los problemas de ciertos delitos informáticos cuya conducta típica no se encuentran muy claros o que no se han llegado a ampliar debidamente; además de que se tienen tipificados algunos ilícitos que no son delitos informáticos en sí, además por otra parte también se presentan los problemas a nivel procesal penal cono judicial, en cuanto que a partir de no realizarse las diligencias periciales de investigación en forma prolija y especializada como se requieren, no se llegan a disponer precisamente de las pruebas periciales competentes, y que por ende los medios probatorios / informáticos requeridos, que se llegan a recaudar resultan en insuficientes y con un reducido valor probatorio, debiéndose a una deficiente cadena de custodia efectuada, o a las demoras que se producen en torno a la ejecución de las pericias correspondientes, además de la sagacidad con que los delincuentes informáticos actúan en borrar o alterar las pruebas que refieren a las pistas, fuentes y medios tecnológicos con que han llegado a perpetrar sus ilícitos informáticos; lo que finalmente provoca que con insuficientes pruebas, los Fiscales Penales del caso no lleguen a formular los ilícitos penales que correspondan al tenerse confusiones sobre qué delito informático es el que corresponde imputar, ya que al tenerse escasos medios probatorios contundentes, finalmente se imputarán a los ciberdelincuentes con otros delitos informáticos de menor penalidad, a los que les debería corresponder originalmente; y que asimismo se haya estado generando la problemática de que numerosos imputados por tales delitos, han llegado a recibir sentencias judiciales con penas condenatorias muy benignas por

tal situación procesal y por la insuficiencia probatoria de los medios de prueba que se llegan a presentar, lo que tiende a producir duda razonable, y que los jueces penales se ven obligados a dar con la aplicación del principio constitucional de in dubio pro reo (Art. 139 Inciso 11 de la Constitución Política de 1993), lo que deviene en que los procesados finalmente reciban penas condenatorias irrisorias por favorecérseles con la imputación de delitos que les favorezcan en la aplicación punitiva de la pena correspondiente, al existir duda razonable al respecto o pleno conflicto de leyes penales; mientras que en el peor de los casos se tienen acerca de los sujetos que son imputados por acceder indebidamente a la información contenida en bases informáticas de datos o al ingresar ilegalmente a correos electrónicos sin autorización alguna, y que en vez de ser procesados por el delito de acceso ilícito a datos informáticos, se les suele imputar finalmente por otros ilícitos como el de violación de la correspondencia tipificado en el artículo 161 del Código Penal vigente, al existir confusión sobre qué tipo penal les correspondería en ser procesados, y de que al existir conflicto de ley penal al respecto, se les ha concedido a tales imputados en ser procesados por un delito de menor gravedad, recibiendo penas suspendidas de prisión menores a 2 o 4 años, lo que resulta totalmente benigno para tales sujetos imputables; y que en el peor de los casos al no tenerse pruebas suficientes, pueden quedar absueltos de toda culpabilidad.

También cabe considerar los problemas delictivos – informáticos que se vienen causando con el uso indebido de herramientas o programas software basados en sofisticados sistemas de inteligencia artificial, que al constituirse en instrumentos para la perpetración de delitos pluriofensivos que afectan a diversos bienes jurídicos protegidos de los ciudadanos; teniéndose en cuanto que afectan convencionalmente a los derechos de la intimidad y privacidad personal de los ciudadanos que resulten vulnerados en su ámbito privado, y hasta pueden ser interceptadas ilegalmente sus comunicaciones y datos personales en sus redes sociales, vulnerándose los bienes jurídicos de la protección del patrimonio y de la seguridad

personal de las víctimas; además de que también puede vulnerarse de manera agravada en forma de atentados contra la vida e integridad de determinadas personas que puedan ser sometidas a seguimientos o reglajes bajo mecanismos tecnológicos de IA como drones programados informáticamente, para que faciliten la perpetración de asaltos, o de que ciertas personas bajo seguimiento electrónico – informático, puedan sufrir así finalmente atentados contra su patrimonio y hasta sobre su propia vida e integridad.

El empleo cada vez más intensificado de herramientas tecnológicas - informáticas altamente sofisticadas por parte de grupos delictivos, que les permite introducirse o injerir sobre la data comunicativa de las personas que lleguen a resultar intervenidas en sus dispositivos de comunicación móvil o hasta resultan ser hackeados en sus redes sociales por elementos inescrupulosos que utilizan programas rutinarios de inteligencia artificial cada vez más especializados, con lo cual aparte de vulnerar la privacidad íntima de los que resultan agraviados en sí, sino que se llega a afectar también de manera directa a la seguridad de las víctimas, que pueden tender a sufrir a su vez asaltos o robos agravados, al tenerse conocimiento indebido sobre los movimientos financieros que va a realizar el individuo que haya sido interceptado en sus comunicaciones y sobretodo de que se le haya hackeado datos esenciales de sus cuentas en red social (twitter, instagram); con lo cual los sujetos delictivos pueden tener altas probabilidades de consumar tales ilícitos; habiéndose para ello accedido ilegalmente a información personal y económica de las víctimas.

La peligrosidad con que se pueden llegar a emplear criminalmente instrumentos altamente sofisticados de Inteligencia Artificial como son los drones, para la comisión de delitos convencionalmente comunes tales como robos y hasta de seguimientos ilegales sobre víctimas potenciales de secuestro o de extorsión, puede acrecentar aún más la problemática de inseguridad ciudadana y de tornarse sumamente complejo para la labor de las Instituciones Públicas - Estatales del proceso penal en dar con la identificación del autor delictivo o de los

sujetos criminales que utilicen tal recurso tecnológico de avanzada, dada la dificultad de poder intervenirse a los delincuentes autores intelectuales que se ocultan y pueden manipular drones a largas distancias para la perpetración de sus fechorías delictivas; y que a lo más la autoridad policial puede llegar a interceptar e incautar equipos electrónicos de drones, más no podrá ubicar e identificar a los elementos delincuenciales como autores criminales de los ilícitos comunes que se lleguen a perpetrar sofisticadamente con el uso tecnológico de drones, lo que podría acrecentar preocupantemente aún más la impunidad de sujetos delincuenciales y de grupos criminales en la comisión de robos y otros ilícitos.

Lo señalado anteriormente se concuerda con lo aportado por los autores Santa Cecilia y González (2019), que consideran:

> De acuerdo a la experiencia de incidencia internacional de casos indebidos o ilícitos de mal empleo de drones para la comisión de acciones dolosas como desórdenes, disturbios o alteraciones públicas, además para la perpetración de atentados contra representantes de autoridades púb1icas, propiamente tratándose de actos terroristas, pero sin dejarse de lado que la utilización indebida de tal medio tecnológico – electrónico de tipo tan sofisticado, también puede ser usado de manera específica por organizaciones delictivas, para dar con el facilitamiento ilícito de perpetración de delitos comunes, como a la vez de tenderse con la impunidad de los sujetos delictivos culpables, por lo que ante ello la legislación penal norteamericana y europea han llegado a contemplar determinadas disposiciones normativas para la tipificación punitiva de delitos comunes perpetrados con el uso de recursos o herramientas tecnológicas, tal como se reconoce y tipifica en torno al artículo 57° bis inciso 1.c del vigente Código Penal español, que llega a considerar punitivamente la aplicación adicional a las penas de prisión básicamente imponibles, la suma de penas adicionales de entre cinco a siete años de cárcel, para todos los sujetos activos que lleguen a perpetrar delitos como robos

y otros ilícitos comunes contra el patrimonio, habiendo utilizado para ello drones o instrumentos tecnológicos de Inteligencia Artificial (pp. 12 - 13).

Asimismo también es importante considerarse sobre determinados casos que se han podido penalizar y asimismo documentar corroborablemente en sentencias desarrolladas por la Jurisprudencia Internacional, y que han quedado como ciertos precedentes, acerca del uso indebido de los drones electrónicos de Inteligencia Artificial, que no pasan desapercibidos para su utilización en la comisión perpetrable de actos delictivos y, que más comúnmente se estén utilizando para la perpetración frecuente de atentados terroristas, son actualmente considerados como amenazas recientes y de peligrosa innovación criminal para la seguridad pública de los países y para todas las personas del mundo, dado los alcances indebidos de uso delictivo como terrorista esencialmente, que se pueden llegar a emplear negativamente a los drones.

Así, la utilización de computadoras en el ámbito multisectorial pero sobre todo en el sector de la banca y seguros, lleva también a la aparición de nuevas formas de delincuencia, representativas del ingenio y la habilidad de estos nuevos "delincuentes de computadoras". De esta manera el mundo, de la informática se convierte, por un lado, en un campo amplio y lleno de posibilidades para el futuro progreso, medio de avance en el desarrollo de la sociedad moderna; pero, por otro lado, se convierte en un factor de "riesgo", en cuanto fuentes de nuevas formas de criminalidad, citando la manipulación de computadoras, la destrucción o alteración de programas, etc.

Por estas razones, se constituyen en antecedente inmediato de la presente investigación, aquellos trabajos de investigación realizados teniendo como objeto de estudio aspectos relacionados con los delitos informáticos y la protección penal de los bienes jurídicos que resultan vulnerados con tales ilícitos, como el patrimonio económico de las personas, el resguardo de la información secreta y hasta la intimidad como privacidad personal de los ciudadanos que resultan vulnerados al respecto. Por ello alcanzaremos en la presente

investigación un instrumento técnico científico de utilidad para los operadores de justicia que actúen sobre la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad (Jueces, Fiscales y Policías) en el Distrito Judicial de Lima y como un aporte para la comunidad científica para encontrar respuestas sobre la problemática actual de acuerdo al uso de tecnología emergente.

1.3. Formulación del problema

1.3.1. Problema general

¿Cómo el tratamiento aplicable de los aspectos sustantivos y procesales sobre imputados por Delitos Informáticos, viene influyendo en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, periodo 2017 – 2018?

1.3.2. Problemas específicos

¿Qué limitaciones se presentan en torno al tratamiento aplicable de los aspectos sustantivos – penales de los delitos informáticos, y cómo influyen sobre la penalización y disminución del cibercrimen en el Distrito Judicial de Lima, durante los años 2017 - 2018?

¿Qué problemas se presentan en torno al desarrollo de los aspectos procesales – penales sobre delitos informáticos, y cómo influyen sobre la penalización y disminución del cibercrimen en el Distrito Judicial de Lima, durante los años 2017 - 2018?

1.4. Antecedentes de la investigación

1.4.1. Antecedentes nacionales

Pardo (2018) en su tesis tuvo como objetivo general analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. Para el cual se utilizó una serie de métodos de investigación, propias de la investigación cualitativa, de nivel descriptivo explicativo. Se utilizó como técnica la entrevista con su respectivo instrumento de recolección de datos, la guía de entrevista, con el cual se recopiló información de los expertos sobre el tema, nacionales y extranjeros, llegándose a conclusiones precisas. En

tal sentido, se concluyó que el tratamiento jurídico penal de los delitos informáticos contra el patrimonio es deficiente, toda vez que ilógicamente se comprende dentro de fraude informático todo los tipos o modalidades de delitos informáticos contra el patrimonio, el cual genera incertidumbre en la interpretación de la norma que no permite la sanción efectiva de los delitos informáticos contra el patrimonio.

Sequeiros (2016) en su tesis de investigación la autora sostuvo que, en los últimos años, producto de la evolución de las tecnologías informáticas se ha ido desarrollando una nueva forma de criminalidad denominada delitos informáticos. En relación a esta nueva forma delictiva, en el Perú se han emitido leyes, cuya finalidad es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datas informáticos, así como los secretos de comunicaciones, y los demás bienes jurídicos que resulte afectado con esta modalidad delictiva como son el patrimonio, la fe pública y la libertad sexual. La Ley N° 30096 "Ley de delitos informáticos" fue promulgada el 21 y publicado el 22 de octubre del 2013 en el diario oficial "El Peruano". Luego fue parcialmente modificada por la Ley N° 30171, promulgada el 9 y publicada el 10 de marzo del 2014. A pesar de ello, algunas conductas desplegadas en el mundo informático, no implica desconocer las ventajas y facilidades brindadas por estos sistemas. Son evidentes los beneficios de los adelantos tecnológicos que trae para la sociedad el uso de la tecnología informática y comunicación. Sin embargo, estos adelantos tecnológicos posibilitan una nueva modalidad de cometer los delitos tradicionales como el fraude y a su vez facilita la comisión de nuevos delitos como la penetración en redes informáticas, el envío de correo basura, la pesca de los datos "pishing", la piratería digital, la propagación maliciosa de virus y otros ataques contra las infraestructuras de información esenciales.

Sánchez (2017) en su investigación tuvo como objetivo principal determinar de qué manera la adopción de estrategias de ciberseguridad incide en la protección de la información en la Oficina de Economía del Ejército, para el cual tuvo como población de estudio a 30

oficiales, 40 técnicos y suboficiales y 180 empleados civiles, teniendo una muestra de 152 participantes, en la que utilizó como técnicas de estudio a la encuesta, entrevista y análisis documental, y como instrumentos de recolección de datos tales como el cuestionario, guía de entrevista y las fichas bibliográficas. El tipo de estudio fue no experimental con diseño transaccional o transversal, nivel de investigación descriptivo y explicativo. Una vez desarrollado los procedimientos metodológicos de la investigación, el estudio concluye que la adopción de estrategias de ciberseguridad incide significativamente en la protección de la información en la Oficina de Economía del Ejército, y entre otras conclusiones señala que en la Oficina de Economía del Ejército no existen planes de protección contra ciberterrortistas y se ponen en ejecución y que los dispositivos con las que cuenta el Ejército no son de última generación, por lo que no se garantiza la protección de la alteración de la información. Entre otras recomendaciones, el autor señala que la Oficina de Economía del Ejército debe tomar acciones legales y disciplinarias para sancionar a quienes coadyuven directa o indirectamente con los actos de los cibercriminales, asimismo, se debe prever y priorizar adquisición de software de última tecnología para el tratamiento o manejo de la información reservada y garantizar la protección efectiva evitando cualquier tipo de alteración.

Alarcón y Barrera (2017) en su investigación tuvo como objetivo general determinar la relación del uso del internet con los delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, seccional Sogamoso, 2016, para el cual utilizaron el tipo de investigación básico, de nivel correlacional, enfoque cuantitativo y el diseño de estudio fue no experimental, cuya población de estudio estuvo conformada por los estudiantes, y tuvieron una muestra de 60 de dichos estudiantes. La técnica de recolección de datos utilizado fue la encuesta y su respectivo instrumento, el cuestionario conformado por 36 preguntas cerradas. En este orden de ideas, el estudio concluye que el uso del internet que implica las competencias informacionales por habilidad, acceso a la información y aspectos

sociales se relacionan con la comisión de delitos informáticos, es decir que la ocurrencia de los delitos informáticos depende del desarrollo de las competencias informacionales en el uso del internet. Finalmente, los investigadores recomiendan que se debe involucrar a los docentes y directivos de las instituciones a que implementen módulos prácticos que permita a los estudiantes alejarse de las prácticas inapropiadas con el uso de la informática, asimismo recomienda concientizar a los estudiantes respecto al uso de la información en la internet.

Prado (2020) sostiene que el ciberespacio, como nueva dimensión de interacción social, política y económica, ha generado un cambio radical en las formas de criminalidad en el Perú. En este entorno digital surgen fenómenos como el fraude informático, la suplantación de identidad, el acceso ilícito a sistemas y la difusión de contenidos ilícitos, que desafían tanto al derecho penal como a las políticas públicas de seguridad. En este sentido resalta el aporte en su obra Delitos informáticos y Derecho Penal en el Perú. Prado desarrolla un análisis detallado sobre la relación entre ciberespacio y ciberdelincuencia, situando el debate en el marco normativo nacional y en los retos procesales de la administración de justicia peruana. El objetivo del trabajo de Prado fue evaluar el alcance del derecho penal peruano frente a los ciberdelitos cometidos en el ciberespacio, tomando como referencia las reformas legislativas derivadas de la Ley N.° 30096 – Ley de Delitos Informáticos (2013) y sus posteriores modificaciones hasta 2019. Su enfoque es claramente dogmático y criminológico, combina la exposición del marco legal con un análisis crítico de su aplicación práctica, revisando además el impacto del Convenio de Budapest sobre Ciberdelincuencia, al cual el Perú se adhirió en 2019. Esto convierte su obra en un referente ineludible para toda tesis doctoral que busque comprender cómo el Estado peruano enfrenta la ciberdelincuencia. Prado identifica que los delitos informáticos regulados en la Ley 30096 se agrupan en tres grandes categorías, i. Los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos (por ejemplo, acceso ilícito, interceptación de datos, interferencia en sistemas), ii. Los delitos

informáticos patrimoniales, que incluyen fraude electrónico, phishing y clonación de tarjetas, iii. Los delitos informáticos vinculados a la intimidad, libertad y dignidad personal, como la pornografía infantil en línea, el grooming y la suplantación de identidad. El autor sostiene que, aunque la ley peruana avanzó en la tipificación sustantiva, aún persisten problemas de técnica legislativa, como la excesiva amplitud de algunos tipos penales y la falta de actualización frente a fenómenos recientes como el ransomware o los delitos relacionados con criptomonedas. En el plano procesal, Prado enfatiza tres problemáticas centrales, i. La prueba digital; Aunque el Código Procesal Penal peruano reconoce la validez de la evidencia electrónica, existe una debilidad en los protocolos de preservación y cadena de custodia, lo cual afecta la eficacia de los juicios. ii. La capacitación de operadores de justicia; La falta de preparación técnica de fiscales, jueces y policías especializados limita la correcta persecución del ciberdelito, generando impunidad en casos complejos, iii. La cooperación internacional; (p. 40). El Perú, al adherirse al Convenio de Budapest, debe implementar mecanismos más ágiles de colaboración judicial, pero en la práctica los trámites de asistencia legal internacional siguen siendo lentos y burocráticos. Prado concluye que la brecha entre norma y aplicación práctica es el principal obstáculo en la lucha contra la ciberdelincuencia en el país.

San Martín (2018) señala que el desarrollo tecnológico y la consolidación del ciberespacio han traído consigo un nuevo escenario para el derecho penal. El Perú no ha sido ajeno a este fenómeno, enfrentando un aumento significativo de conductas ilícitas en entornos digitales, que van desde fraudes electrónicos hasta delitos contra la intimidad y la dignidad personal. La necesidad de adaptar la ley penal a estos desafíos ha impulsado reformas legales como la Ley N.º 30096 – Ley de Delitos Informáticos (2013), modificada en 2014 y objeto de interpretación jurisprudencial en años posteriores. En el contexto de este fenómeno, resalta el trabajo del jurista San Martín Castro, magistrado supremo y catedrático universitario, quien en 2018 publicó artículos y ponencias donde analiza la cibercriminalidad y el derecho penal,

destacando la tensión entre las nuevas tipologías delictivas y los principios clásicos del ius puniendi. Sus reflexiones constituyen un precedente fundamental que buscan explorar cómo la ley penal peruana se ha adecuado frente a la criminalidad digital. El análisis de San Martín, tuvo como objetivo central examinar la incorporación de los delitos informáticos en el derecho penal y su coherencia con los principios de legalidad, proporcionalidad y mínima intervención penal. Asimismo, buscó evaluar los problemas prácticos derivados de la aplicación judicial de la Ley N.º 30096, especialmente en lo que concierne a la prueba digital y a la interpretación de los tipos penales. Desde el plano sustantivo, San Martín sostiene que la Ley de Delitos Informáticos peruana representó un avance normativo importante, al tipificar conductas como; Acceso ilícito a sistemas y datos, Interceptación de datos informáticos, Fraude electrónico y suplantación de identidad, Pornografía infantil en línea y grooming. Sin embargo, advierte que varios de estos tipos penales fueron redactados con técnica legislativa deficiente, lo que genera problemas de interpretación en sede judicial. Por ejemplo, figuras como el "acceso ilícito" o la "interceptación" poseen descripciones amplias que pueden vulnerar el principio de taxatividad penal. Asimismo, San Martín reflexiona sobre el bien jurídico protegido en estos delitos. Mientras algunos sostienen que la protección recae en la intimidad o la propiedad, él plantea que en muchos casos lo que se tutela es la seguridad de la información como un nuevo bien jurídico autónomo, lo cual representa un cambio de paradigma en la dogmática penal. En lo procesal, el autor resalta la dificultad de aplicar el derecho penal clásico a un entorno caracterizado por la volatilidad y transnacionalidad de la prueba digital. Identifica tres retos, i. la cadena de custodia; La evidencia digital puede ser alterada fácilmente, y los protocolos peruanos aún carecen de la solidez técnica necesaria para garantizar su fiabilidad en juicio, ii. La competencia territorial; Muchos ciberdelitos trascienden fronteras, pero la legislación procesal peruana mantiene un enfoque estrictamente territorial, lo que genera problemas de jurisdicción, iii. La capacitación judicial; Fiscales y jueces muestran limitaciones en

conocimientos técnicos sobre sistemas informáticos, lo cual dificulta la adecuada valoración de la prueba. Además, concluye que sin una reforma procesal y una mejor formación de los operadores de justicia, el derecho penal peruano seguirá siendo ineficaz frente a la ciberdelincuencia.

1.4.2. Antecedentes internacionales

Abdulai (2016) en su investigación tuvo como objetivo de estudio investigar el miedo a la victimización por delito cibernético (fraude con tarjeta de crédito / débito) entre los estudiantes de la Universidad de Saskatchewan. Los hallazgos del estudio indican que la experiencia previa de victimización y los comportamientos de uso de Internet están asociados positivamente con el miedo de los estudiantes y su riesgo de convertirse en víctimas de fraude con tarjeta de crédito / débito. Por otro lado, se descubrió que los factores sociodemográficos y el conocimiento del delito cibernético son predictores no significativos del miedo y el riesgo de los estudiantes, y de la experiencia de la victimización y los comportamientos de uso de Internet. En términos generales, el estudio encontró que la experiencia de victimización y los comportamientos de uso de internet están asociados positivamente con el temor de los estudiantes y su riesgo de convertirse en víctimas de fraude con tarjetas de crédito / débito. Asimismo, se encontró que los factores sociodemográficos no predicen significativamente el temor a la victimización por fraude con tarjetas de crédito / débito. Es decir, la identificación sociodemográfica de los estudiantes no estaba relacionada con su temor a la victimización por fraude con tarjetas de crédito / débito.

Wang (2016) en su investigación cuyo objetivo fue hacer un estudio comparativo de la ciberdelincuencia de los países China, Estados Unidos, Inglaterra, Singapur y el Consejo de Europa. En tal sentido, entre sus conclusiones señala que China tiene un sistema de regulación de niveles múltiples en malas acciones cibernéticos, con el de los instrumentos básicos y principales y sus dos enmiendas. Aunque ambas dos Enmiendas han llegado a ampliar el

alcance de los delitos informáticos, las razones de expansiones eran diferentes. La Enmienda (VII) se publicó en 2009 para cubrir la brecha que se levantó junto con la creciente popularidad de los ordenadores personales. Después de esta modificación, se estableció el enfoque de dos puntos y una dimensión. Este enfoque hace una clara distinción entre el delito informático genuina (es decir, los delitos que tienen como objetivo la seguridad del sistema de información de la computadora y los datos) y los delitos tradicionales facilitados por computadoras (es decir, delitos en virtud de las disposiciones penales tradicionales). Señala que en los EE.UU. pese a que logra penalizar las malas acciones cibernéticos no está exenta de problemas. Una preocupación importante es su actitud hacia el equipo y los datos. En los delitos de piratería los legisladores eligen una perspectiva estrecha y proteger la seguridad de la computadora; mientras que en otros delitos como el tráfico de dispositivos, las secciones relacionadas se basan en el concepto de datos e información. A partir 19 de estos dos puntos de vista en consideración, la gente puede encontrar la legislación de los Estados Unidos sobre la ciberdelincuencia menos consistente, y esa incompatibilidad conduce a problemas en la práctica judicial. Inglaterra opta por introducir nuevas disposiciones y actos que se actúe con los 'genuino ciberdelincuencia' y se basan en sus disposiciones penales existentes que se ocupan de los delitos tradicionales facilitados por computadoras. Este enfoque, como sugiere la Comisión de Derecho, se llama el enfoque 'a medio camino', lo que significa que 'rechazar la creación de completamente nuevos delitos, excepto cuando éstos son absolutamente necesarios, pero se debe estar preparado para contemplar la ampliación de los delitos generales existentes. Considera que Singapur ha sido activo en la promulgación y modificación de su Ley sobre Abusos Informáticos.

Alanezi (2015) en su investigación cuyo objetivo fue examinar las contramedidas empleadas por las instituciones financieras en Arabia Saudita y el impacto de las contramedidas de forma individual y colectiva en el control y prevención del fraude en línea en Arabia Saudita.

Señala que las personas son dependientes de Internet; la posibilidad de ser violado por los hackers y estafadores está creciendo, especialmente en lo que la socialización, compras en línea y la banca se llevan a cabo a través de computadoras personales o dispositivos móviles. El fraude en línea ha sido descrito como una epidemia que se ha extendido a la mayoría de las actividades en línea. Su prevalencia se ha observado que en las regiones donde hay un alto nivel de adopción del comercio electrónico, y, junto con él, grandes transacciones financieras en línea. Por lo tanto, el argumento es que las medidas tomadas o son insuficientes o no han podido hacer frente con eficacia todos los problemas a causa del contexto organizacional y ambiental del país. La investigación fue de enfoque cualitativo, técnica de entrevista a expertos, la población del estudio estuvo conformada por doce grandes instituciones financieras de Arabia Saudita, incluyendo bancos y otras organizaciones que prestan servicios financieros, en especial los departamentos de Tecnología de la Información, departamentos de comercio electrónico y servicios de gestión de riesgos de los bancos más importantes.

Rincón (2015) en su investigación tuvo como objetivo de investigación proponer la base de una elaboración teórica desde la dogmática penal internacional que permita discutir sobre la necesidad de incluir la investigación y juzgamiento de los delitos informáticos, electrónicos y de las telecomunicaciones en la competencia del Estatuto de Roma, en tal sentido señala que el uso de las tecnología y la racionalidad de la ciencia supo crear un nuevo paradigma con el cual el ser humano entró en una nueva época, de modo tal que el conocimiento y tecnología se convierten, rápidamente, en el mejor aliado de la producción de riqueza. Señala que el "problema del fraude internacional ha sido planteado por diversos sectores de la sociedad internacional, desde organizaciones internacionales hasta empresas transnacionales", como por ejemplo la empresa McAfee, sustentado en información del FBI y la inteligencia europea en diciembre de 2006 publicitado por la Asociación de Internautas, se señala que una de las causas

del auge del cibercrimen en Europa del este, es el alto grado de desempleo y de los bajos salarios, muchos de esos cibercriminales ven internet como una oportunidad de empleo.

Bandler & Merzon (2020) los Exfiscales especializados en cibercrimen brindan una visión holística y práctica sobre cómo se abordan los aspectos sustantivos, pues definen claramente los delitos cibernéticos como conductas tipificadas como ilícitas, por ejemplo, acceso no autorizado, fraude informático, interceptación, etc. Sitúan estos delitos en el contexto legal moderno y explican la fundamentación jurídica para su criminalización, así como los bienes jurídicos protegidos. Procesalmente, dedican secciones a la recolección de evidencia digital, herramientas como órdenes judiciales, preservación de datos, interceptación, técnicas de investigación forense digital. Además, incluyen perspectivas desde la policía, el sector privado y reguladores sobre cómo se llevan a cabo las investigaciones, identificación de sospechosos, aprehensiones y litigación tanto en sede penal como civil o regulatoria. Visiones específicas en la persecución del delito informático.

Fernández et al. (2019) en el marco de una criminología digital centrada en comprender los actores detrás de la ciberdelincuencia, llevaron a cabo un estudio pionero en el contexto hispano, enfocado en el perfil psicosociológico del ciberdelincuente. El propósito fue identificar y describir los posibles perfiles existentes de ciberdelincuentes desde una perspectiva psicosocial. Para ello, se delimitan arquetipos típicos, se consideran variables como edad, género, motivaciones y se contraponen con los contextos de ciberterrorismo y ciberguerra, resaltando además la carencia de estudios en esos ámbitos. El estudio adopta una metodología cualitativa, basada en revisión documental y análisis conceptual, permitiendo perfilar a los actores criminales más recurrentes en el ciberespacio, sin apoyarse en encuestas empíricas masivas, pero consolidando categorías heurísticas útiles para investigaciones posteriores. En cuanto a los arquetipos y características del ciberdelincuente, los autores detallan varios arquetipos del ciberdelincuente, destacando los siguientes perfiles: i. Hacker

idealista o moralista: individuos que vulneran sistemas informáticos motivados por ideales políticos, sociales o éticos. Aunque sus acciones son ilícitas, se justifican en la denuncia de vulneraciones o la lucha contra el sistema; ii. Delincuente oportunista o fraudulento: caracterizado por la búsqueda de ganancias económicas fáciles, mediante fraudes, phishing, e-commerce ilícito, robo de datos; iii. Ciberterrorista o agente ideológico: perfil que incorpora organizaciones o individuos que emplean medios digitales para desestabilizar, coaccionar o difundir mensajes de violencia política o social; a pesar de su relevancia, los autores advierten que este perfil requiere mayor investigación, dada la escasez de datos empíricos; iv. Actor en ciberguerra: usualmente vinculado a estados o grupos estructurados que participan en espionaje o sabotaje digital. El estudio señala que aún hay una brecha investigativa en torno a su perfil psicosocial, pese a su creciente presencia en los escenarios contemporáneos. Además, se discuten rasgos comunes como el uso intensivo de tecnología, bajo nivel de regulación emocional frente a actividades ilícitas, y motivaciones mixtas (ideológicas y lucrativas), aunque estas generalizaciones requieren validación empírica. En cuanto a la innovación temática; aporta una mirada psicosociológica al estudio de la ciberdelincuencia, permitiendo abordar la conducta delictiva digital desde variables individuales y sociales, no solo técnicas o legales. Ergo la construcción de perfiles arquetípicos; establece un punto inicial sólido para operacionalizar variables en futuras investigaciones, por ejemplo, mediante encuestas o entrevistas a actores jurídicos o víctimas. De otro lado respecto a la identificación de vacíos; el reconocimiento explícito de lagunas, especialmente en el estudio del ciberterrorismo y ciberguerra desde lo psicosocial, orienta nuevas líneas de investigación. Profundizar en los factores motivacionales, estructurando una tipología cuantitativa de motivaciones (económicas, ideológicas, psicológicas) y relacionándolas con variables sociodemográficas. Finalmente evaluar los desafíos metodológicos de estudiar perfiles en redes cerradas o en el

anonimato del ciberespacio, proponiendo herramientas mixtas que combinen análisis forense digital y perspectiva criminológica.

Brenner (2017) en su texto Cybercrime and the Law: Challenges, Issues, and Outcomes, indica que el crecimiento de la cibercriminalidad en la última década ha transformado los paradigmas del derecho penal contemporáneo. En un entorno caracterizado por la transnacionalidad de los delitos, el anonimato en redes y la complejidad de la evidencia digital, los juristas internacionales se han visto obligados a replantear las bases de la dogmática penal y los mecanismos procesales de persecución. En este contexto, la obra resulta influyente, pues ofrece una visión profunda sobre cómo los delitos informáticos tensionan los principios tradicionales del derecho penal, al tiempo que plantea respuestas normativas y procesales adaptadas a la era digital. El objetivo central de la obra de Brenner es examinar los desafíos que la cibercriminalidad impone al derecho penal sustantivo y procesal, identificando las limitaciones de las legislaciones nacionales y destacando la necesidad de marcos internacionales de cooperación. Brenner desarrolla su análisis con ejemplos de jurisprudencia estadounidense y casos emblemáticos, pero también incorpora referencias comparativas al Convenio de Budapest sobre Ciberdelincuencia, lo cual le da una proyección global. En cuanto al derecho penal sustantivo, el autor argumenta que la tipificación de los delitos informáticos presenta tres problemas centrales; i. Una elasticidad del tipo penal; Los delitos tradicionales de fraude, robo o daño a la propiedad no abarcan plenamente las conductas digitales, lo que obliga a legislar figuras específicas como acceso ilícito, sabotaje informático o phishing, ii. El principio de legalidad; La rápida evolución tecnológica genera un rezago legislativo. Según el autor, muchas conductas quedan en un "área gris" donde los jueces deben interpretar extensivamente la ley, corriendo el riesgo de vulnerar la seguridad jurídica; iii. El bien jurídico protegido. Se debate si los delitos informáticos tutelan la propiedad, la intimidad, la seguridad de la información o incluso la confianza en el ciberespacio como bien jurídico autónomo.

También destaca la aparición de delitos híbridos, donde lo informático es solo un medio para vulnerar bienes tradicionales (fraudes bancarios, extorsión digital), lo cual exige un enfoque integral del derecho penal. Desde la perspectiva procesal, se enfatiza cuatro ejes problemáticos; i. La obtención de evidencia digital; La dificultad de preservar la cadena de custodia de datos volátiles que pueden ser eliminados o alterados con facilidad, ii. La jurisdicción; Un delito puede iniciarse en un país y culminar en otro, generando conflictos de competencia. La autora subraya que el derecho penal clásico, de base territorial, resulta insuficiente frente a la naturaleza global de Internet, iii. La cooperación internacional; La efectividad de las leyes penales depende de tratados bilaterales o multilaterales, siendo el Convenio de Budapest el principal instrumento, aunque no adoptado universalmente, iv. Los derechos fundamentales; Brenner advierte sobre los riesgos de que la persecución del cibercrimen erosione derechos como la privacidad y la libertad de expresión, especialmente con técnicas intrusivas de vigilancia digital.

Por su parte, Bustos y Zúñiga (2013) en su tesina de investigación, en que procedieron a analizar acerca de la tipicidad de los delitos informáticos en el derecho penal chileno y en el penal comparado; donde precisan que el brevísimo contenido tipificador de la Ley Penal Chilena basada en la Ley N° 19.223 de fecha 07 de junio de 1993 sobre la tipicidad de determinadas modalidades de delitos informáticos, no llega a propiciar sobre poder reconocerse a la amplia variedad de bienes jurídicos que son afectados por dichos delitos, entre ellos el de la intimidad personal, ya que las cuatro figuras delictivas contempladas en la ley penal mencionada, solo hacen referencia a la afectación de los datos contenidos en sistemas y programas informáticos, que pueden ser vulnerados por las acciones delictivas de destrucción o inutilización maliciosa de un sistema informático o de sus partes o componentes, por interceptación o interferencia indebida, por alteración ilegal de datos informáticos, y hasta por los actos de divulgación o revelación no autorizada de datos obtenidos ilícitamente de sistemas

informáticos; lo que da constatación de que mayormente se llega a contemplar con la tipificación de los ilícitos referidos, de que solamente se está vulnerando el bien jurídico basado en la información almacenada en sistemas informáticos, sin considerarse por la legislación penal chilena al respecto sobre la afectación que también se pueda generar sobre el bien jurídico de la intimidad de las personas por propia causa comisiva de los ilícitos informáticos que vulneren la privacidad de las personas naturales, al accederse y obtenerse indebidamente sus datos personales, así como de imágenes y videos de estricta confidencialidad privada/personal de los ciudadanos afectados, siendo que general y básicamente la ley penal chilena contra delitos informáticos solamente se aborda la tipificación de los ilícitos informáticos que vulneren la integridad y seguridad de los datos almacenados en sistemas informáticos pertenecientes directamente a personas jurídicas o empresas, que pueden ser víctimas de actos de sabotaje informático de parte de delincuentes informáticos o por parte de grupos criminales de hackers informáticos, pero no se hace mención particular en la Ley N° 19.223 sobre los delitos informáticos que explícitamente vulneren la intimidad de las personas, ya que meramente se tiene sobre aquello a lo tipificado en el Código Penal Chileno de 1874 actualizado al 2018, que tipifica a los delitos contra la intimidad personal generalizadamente por todos los medios informáticos y otros posibles que permitan grabar y reproducir conversaciones privadas como también imágenes y videos de estricto carácter confidencial privado – íntimo; tratado tácita o indirectamente en base a lo tipificado entre los artículos 161 – A y 161 – B del referido Código Punitivo Chileno; mientras que a diferencia de lo tratado en la legislación penal comparada de países como Francia, Alemania y España, donde sí se llega a considerar la tipicidad específica de los delitos informáticos que afecten la intimidad de las personas, y estableciendo para ello sanciones punitivas drásticas en sí, aunque de manera delimitada en el caso del Código Penal Español que aplica penas benignas sobre tales ilícitos informáticos.

Wall (2017), criminólogo británico cuya obra Cybercrime: The Transformation of Crime in the Information, destaca la expansión del ciberespacio como entorno global de interacción humana, económica y política ha redefinido el campo de la criminalidad. En este nuevo escenario, la ciberdelincuencia se manifiesta como una de las expresiones más complejas de la criminalidad moderna, por su capacidad de cruzar fronteras, explotar vulnerabilidades tecnológicas y desafiar los marcos normativos clásicos. ha tenido múltiples reediciones y actualizaciones. Asimismo, profundiza en la intersección entre ciberespacio y ciberdelincuencia, abordando tanto las transformaciones estructurales que la red global genera sobre la delincuencia, como las respuestas legales y criminológicas. El propósito de esta investigación fue explicar cómo el ciberespacio altera la naturaleza de la criminalidad y cómo ello exige repensar la aplicación del derecho penal y los modelos criminológicos. Para el autor, el ciberespacio no es simplemente un nuevo escenario, sino un espacio de transformación que cambia las motivaciones, oportunidades y formas de comisión delictiva. El enfoque adoptado combina elementos de criminología, sociología del derecho y estudios de seguridad digital, lo que ofrece una perspectiva interdisciplinaria que enriquece los estudios jurídicos. De esta manera, el autor no se limita a la mera descripción de delitos informáticos, sino que plantea cómo el propio concepto de delito se ve transformado en un contexto digitalizado. Argumenta que el ciberespacio es un territorio híbrido, caracterizado por tres elementos; i. La deslocalización. La conducta delictiva puede originarse en un país, ejecutarse desde otro y tener víctimas en varios lugares distintos, lo que desafía los marcos tradicionales de soberanía y jurisdicción penal, ii. El anonimato y multiplicación de identidades. El uso de redes privadas, encriptación y pseudónimos permite que los ciberdelincuentes operen sin una identidad clara, lo cual dificulta la atribución de responsabilidad penal, y iii. La Velocidad y masificación. A diferencia del delito físico, el ciberdelito puede ejecutarse en segundos y afectar simultáneamente a miles de víctimas en diferentes regiones del mundo. Estos rasgos convierten

al ciberespacio en un ámbito que no solo facilita nuevas formas de criminalidad, sino que también reconfigura las estructuras de poder, control y vigilancia; En cuanto a la ciberdelincuencia, Wall sostiene que esta puede clasificarse en tres niveles, i. El cibercrimen como nuevo delito; conductas que solo existen en el entorno digital, como la creación y distribución de malware, ataques de denegación de servicio o ransomware, ii. El cibercrimen como extensión de delitos tradicionales, por ejemplo, fraude, robo de identidad o acoso, que en el ciberespacio adquieren nuevas modalidades y mayor escala, iii. El cibercrimen como crimen organizado transnacional: grupos criminales que operan profesionalmente en el ciberespacio, con estructuras jerárquicas y roles definidos, aprovechando mercados negros en la Dark Web. Este análisis permite entender cómo la ciberdelincuencia no es un fenómeno homogéneo, sino que varía según los actores, las motivaciones y los medios tecnológicos empleados. Asimismo, desde el punto de vista penal, Wall destaca tres desafíos principales; i. Una tipificación adecuada; Los códigos penales nacionales suelen quedarse rezagados frente a la innovación tecnológica, generando vacíos legales que impiden perseguir conductas nuevas, ii. Una jurisdicción y cooperación internacional; El derecho penal tradicional, de base territorial, se ve superado por la transnacionalidad de los ciberdelitos. Por ello, Wall enfatiza la necesidad de marcos como el Convenio de Budapest y de mecanismos más ágiles de asistencia legal mutua, iii. Una protección de derechos fundamentales; El combate a la ciberdelincuencia requiere medidas intrusivas (vigilancia digital, interceptación de datos, uso de inteligencia artificial), lo que plantea un equilibrio delicado entre seguridad y respeto a la privacidad, libertad de expresión y debido proceso.

1.5. Justificación de la investigación

Es la conformidad y lo justo en la vida de las personas y las cosas. Siendo así, el presente trabajo de investigación pretende justificar teniendo en consideración, el factor determinante que contribuye a la eficiencia de la labor de los operadores de justicia (Policías, Fiscales y

Jueces) comprometidos con la investigación y juzgamiento de los delitos informáticos y la protección penal del patrimonio, lo cual posibilitará mejorar el tratamiento de la problemática en el Perú. Ya que tanto el derecho de la información como el derecho de la vida privada, forman parte de los llamados derechos humanos o fundamentales. Por tanto, este trabajo de investigación se justifica porque:

- Es insuficiente la investigación sobre el tema en particular y con la presente investigación se llenarán esos vacíos de información.
- Con los resultados obtenidos de esta investigación se beneficiarán los operadores de justicia y la población en general.
- Con las escasas investigaciones que se realizaron en los niveles académicos que son solo a estudios superficiales descriptivos sobre el tema, con esta investigación se plantearan opciones de solución al problema de identificación y descripción.
- Se tendrán condiciones de hacer las recomendaciones tendientes a seguir adecuando el marco teórico de acuerdo a los cambios de modalidades de los delitos informáticos.

Como bien se sabe, la tecnología informática representa el principal avance de fines del siglo XX e inicios del siglo XXI. Nunca antes, la humanidad estuvo tan interrelacionada y comunicada como ahora lo está. La prueba más fehaciente la encontramos en el uso de Internet, que representa, de acuerdo Bill Gates, la supercarretera mundial, donde mujeres y hombres de todos los países, condiciones e ideologías, se interrelacionan y comunican, dando paso a la globalización y al mismo tiempo, a lo que se ha denominado la aldea global.

1.5.1. Justificación práctica

Así como la tecnología avanza, la delincuencia también lo hace, aprovechando las redes y espacios informáticos, para afectar los bienes jurídicos y para dañar la integridad (salud mental y emocional), honor, patrimonio, propiedad intelectual, fe pública, libertad sexual, entre otros bienes jurídicos. Los delincuentes informáticos, a nivel nacional, son muy hábiles para

cometer dichos delitos y evitar ser reconocidos, toda vez, que los indicios y evidencias en las computadoras y ordenadores, pueden desaparecerse o borrarse, de tal manera, que no se puede acreditar el ilícito penal.

Como bien observamos, según los reportes e informes de la PNP y el Ministerio Público, los delitos informáticos que más se cometen son la promoción de la prostitución infantil (proxenetismo) y la difusión de la pornografía infantil, lo que constituye una ofensa al pudor público, lo más grave es que se atenta contra los derechos del niño y del adolescente. Los pederastas y los pedófilos cometen estos delitos con la mayor impunidad y se valen del Chat para captar a sus víctimas, habiendo al mismo tiempo, acumulado cantidad de material pornográfico en sus domicilios o lugares donde reúnen el material aludido, tal como se desprende de los reportajes difundidos por los medios de comunicación.

También tenemos el caso de la utilización de los soportes informáticos para realizar reproducciones y copias ilegales de obras y creaciones protegidas por la ley de propiedad intelectual. Conocemos que, a nivel nacional, la venta de los denominados CDs piratas se ha incrementado. Al respecto, son miles, las copias que se venden y ofertas que se venden en las calles, no existiendo una adecuada prevención, investigación y lucha contra esta modalidad delictiva.

Los adelantos de la tecnología informática han posibilitado en nuestro país avances y progreso en los negocios, en la vida académica, familiar, social, política y cultural. Sin embargo, también es utilizado por la delincuencia y criminalidad para atentar contra los bienes jurídicos, utilizando los soportes y ordenadores informáticos, cometiéndose delitos contra el patrimonio, contra la libertad sexual, contra la fe pública, contra la propiedad intelectual, etc.

Asimismo se debe tener en cuenta que el crimen cibernético se viene constituyendo cada vez de gran riesgo para la seguridad nacional de todo Estado, y más inclusive para la seguridad y defensa nacional del Perú, considerando el grave riesgo y las implicancias que

tendrían que hackers o grupos de ciberterroristas – espías informáticos nacionales o extranjeros accedan a información confidencial de los sistemas de defensa de las instituciones armadas nacionales; podría generar que países interesados y que compiten geoestratégica y militar contra nuestro país (caso de Chile) y hasta inclusive organizaciones criminales, pueden llegar a obtener información reservada de Defensa Nacional a fin de traficarla y venderla a mejores postores extranjeros, lo que de ser manipulada y usada dicha información contra los intereses nacionales, ya se constituye en una grave afectación a la seguridad y soberanía del Perú. Nuestro país ya viene adoptando las medidas legales, jurídicas y de cooperación inter-institucional a nivel policial como en Sector de Defensa para luchar y neutralizar toda amenaza del crimen cibernético, dada la potencialidad amenazante que tienen grupos terroristas como Anonymus para acceder a cualquier sistema informático, asimismo de las acciones de espionaje que realizan agentes militares secretos y privados de EE.UU. (Caso Assange), además de los ataques cibernéticos de Hackers Chilenos que han manipulado y alterado el normal funcionamiento de la página web del Ministerio de Defensa, y de la amenaza global que significa las Unidades Hackers del Ejército de China que pueden vulnerar cualquier sistema informático y acceder a información reservada de Defensa y Seguridad de cualquier país.

El Crimen Cibernético también se viene constituyendo en una herramienta valiosa para las grandes organizaciones criminales transnacionales dedicadas al narcotráfico y a delitos que se perpetran traspasando las fronteras de diversos países de la región; teniendo en cuenta la experiencia de las FARC's colombianas que disponían de Comandos para realizar ataques cibernéticos a las páginas web de las Fuerzas Militares Colombianas, a fin de ocasionar desinformación, y usar canales del ciberespacio para la ejecución de sus operaciones de tráfico de drogas y lavado de activos en conexión con organizaciones narcotraficantes de México; mientras que en este último país los Cárteles de la Droga disponen de grupos de hackers contratados para acceder a información confidencial de los sistemas informáticos de las

autoridades policiales mexicanas tanto para sabotear las bases de datos policiales y hasta de conocer las estrategias operativas para anticipar el accionar policial, además del acceso a información privada de los funcionarios policiales como de informantes para después atentar contra la vida e integridad de los mismos; teniéndose así que si bien en el caso peruano no se llegan a dimensiones agravantes del crimen cibernético que se está perpetrando de manera que atenta principalmente contra el patrimonio económico de usuarios y empresas conectados en el ciberespacio, pero cada vez más hackers nacionales y el uso de herramientas informáticas sofisticadas y elaboradas en mercados clandestinos (caso de la venta de software informal y de acceso a información secreta de funcionarios y miembros de empresas privadas, que se trafica ilegalmente en las Galerías de la Avenida Wilson – Centro de Lima), así como el caso de espías de nuestras propias FF.AA. teniéndose el caso emblemático del ex – Sub Oficial FAP Víctor Ariza que en el 2009 suministró a fuentes militares chilenas, información secreta de Defensa de la FAP siendo condenado a 25 años de prisión por delito de espionaje; no descartándose hasta el momento de que el condenado haya empleado técnicas de espionaje informático y hasta de haber estado asociado con grupos delictivos de ciber-espías para acceder a información tan relevante y altamente secreta de la Fuerza Aérea Peruana. Se tiene así que por todos estos elementos mencionados que ocurren y se han dado en nuestro país, existe potencialmente riesgos para que la criminalidad cibernética se consolide atentando contra la seguridad nacional.

1.5.2. Justificación Doctrinaria – Dogmática

El desarrollo de la investigación se justificó desde el punto de vista doctrinario por cuanto es necesario actualizar la doctrina y las categorías conceptuales sobre los delitos informáticos, habida cuenta de que, tras 5 años y medio de vigencia de tales delitos tipificados en la Ley N° 30096 del 2013 y acorde con su última modificatoria basado en la Ley N° 30171 del 2014; se necesita esencialmente de una fundamentación doctrinaria penal exhaustiva y

rigurosamente sustentable sobre la interpretación de dichos ilícitos acorde a lo tipificado en la Normatividad Penal, a efectos de poderse sustentar los aspectos sustantivos de tales ilícitos, de manera completa, exhaustiva y sin problemas de vacíos legales; y que asimismo contándose con los fundamentos dogmáticos y casuísticos - prácticos necesarios se pueda facilitar a los operadores jurídicos – procesales (Fiscales y Jueces Penales) de que puedan llegar a contar con toda la fundamentación requerida para que puedan sustentar los alegatos con que deban fundamentar las denuncias penales que deben interponerse contra autores por comisión de delitos informáticos, y asimismo para fundamentarse las órdenes o mandatos fiscales de prisión preventiva y de otras medidas coercitivas sobre imputados por grave comisión de dos o más ilícitos informáticos en forma de crimen organizado.

Además de que con los fundamentos dogmáticos – doctrinarios en que se pueda fundamentar ampliamente cada delito informático tipificado en la Ley N° 30096 y su modificatoria basada en la Ley N° 30171, concordado con la casuística jurisprudencial pertinente, en que se amplíe y fundamente sobre la tipicidad penal en torno a los aspectos objetivo y subjetivo de derecho penal sobre cada ilícito, y asimismo sobre la ejecución de los mecanismos y diligencias procesales – penales en que deben tratarse y resolverse procesalmente los casos imputables de ilícitos informáticos de manera efectiva y con la mayor celeridad posible, que los jueces penales puedan así formular y explicar los fundamentos de derecho y de interpretación de la norma penal correspondiente en sus sentencias judiciales, en cuanto a la aplicabilidad requerida sobre el caso de ilícito informático procesado judicialmente; para su tratamiento procesal y resolución efectiva por la instancia judicial pertinente.

1.5.3. Justificación jurídica

Frente a la problemática que representa el crimen cibernético, nuestro país ya dispone de una legislación penal preventiva y disuasiva para penalizar todo tipo de delito informático que se perpetre en cualquiera de sus modalidades, y más aún si llega a atentar contra la

seguridad y defensa nacional; teniéndose así lo ya tipificado en el Código Penal con respecto a los delitos informáticos en sus modalidades convencionales de comisión tipificados entre los Artículos 207 – A al 207 – C, además del delito de espionaje tipificado en el Art. 331 - A, y asimismo en lo que corresponde a los delitos informáticos específicamente tipificados en la Ley 30096 (Ley Actual de Delitos Informáticos - LDI) del 2013 que es muy importante porque ha regulado todo sobre los delitos informáticos que pueden afectar directa o indirectamente la seguridad y defensa nacional de nuestro país.

Gran parte del catálogo vigente de delitos informáticos anterior a la LDI data del año 2000 y tenía como bien jurídico protegido el patrimonio (Título V, Capítulo X del Código Penal). Cabe referirse a los artículos 207-A (espionaje o intrusismo informático), 207-B (sabotaje informático) y 207-C (agravantes). El espionaje o intrusismo informático sancionaba la utilización o ingreso subrepticio a una base de datos, sistema o red de computadoras o cualquier parte de la misma para diseñar, ejecutar o alterar un esquema u otro similar. La pena máxima era 2 años de cárcel. El sabotaje informático sancionaba la utilización, ingreso o interferencia a una base de datos, sistema, red o programa de ordenador con la finalidad de alterarlos, dañarlos o destruirlos. La pena máxima era 5 años de cárcel. Los agravantes sancionaban con 7 años de cárcel a quienes cometían espionaje o sabotaje informático cuando el agente ingresaba a la base de datos, sistema o red de computadoras haciendo uso de información privilegiada en función a su cargo o ponía en riesgo la seguridad nacional (pena máxima de 7 años de cárcel).

El 19 de agosto de 2013 la Ley 30076, incorporó un nuevo delito: el tráfico ilegal de datos sancionando a aquel que “crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral o financiera.

1.6. Limitaciones de la investigación

Las limitaciones en esta investigación, fueron las referentes a trabajos anteriores de investigación, hay pocos libros, poco material de consulta, pocas publicaciones y bibliografía. Sin embargo, hemos encontrado mucha colaboración para dilucidar este problema a nivel de los operadores jurídicos. Son escasos los especialistas al respecto, y las autoridades prestan nulo o escaso apoyo para este menester.

Hay insuficiente información virtual que nos haga pensar que a nivel internacional se haya visto este mismo problema.

Es cierto que tradicionalmente se haya centrado este discurso en la pena, en sus funciones y fines, conviene no perder de vista que en la fase de individualización de la pena se despliegan series de consecuencias penales y eventualmente civiles que intentan responder al complejo de demandas sociales que se articulan frente al delito cometido, más aún cuando éste posee un carácter de dañino relevante.

1.7. Objetivos

1.7.1. Objetivo general

Explicar acerca del tratamiento aplicable de los aspectos sustantivos y procesales sobre imputados por Delitos Informáticos, y cómo viene influyendo en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, periodo 2017 – 2018.

1.7.2. Objetivos específicos

Explicar las limitaciones que se presentan en torno al tratamiento aplicable de los aspectos sustantivos – penales de los delitos informáticos, y cómo influyen sobre la penalización y disminución del cibercrimen en el Distrito Judicial de Lima, durante los años 2017 - 2018.

Explicar los problemas que se presentan en torno al desarrollo de los aspectos procesales – penales sobre delitos informáticos, y cómo influyen sobre la penalización y disminución del cibercrimen en el Distrito Judicial de Lima, durante los años 2017 - 2018.

1.8. Hipótesis

1.8.1. Hipótesis general

Los constantes problemas en el tratamiento aplicable de los aspectos sustantivos y procesales sobre imputados por Delitos Informáticos, influyen negativamente en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, durante los años 2017 – 2018.

1.8.2. Hipótesis específicas

Las limitaciones de vacíos legales y deficiencias que se presentan en torno al tratamiento aplicable de los aspectos sustantivos – penales de delitos informáticos, influyen negativamente en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, durante los años 2017 – 2018.

Los problemas de insuficiencia de métodos y criterios procesales - jurídicos de parte de los Operadores de Derecho Penal, que se presentan en torno al desarrollo de los aspectos procesales – penales, influyen negativamente en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, durante los años 2017 – 2018.

II. MARCO TEÓRICO

2.1. Marco conceptual

Acceso Ilícito. El hecho de ingresar o la intención de ingresar sin autorización, o a través del acceso de un tercero, a un sistema de información, permaneciendo o no en él.

Afectar. Alterar, provocar anomalías en cualquiera de las operaciones a realizar por un programa, software, sistema, red de trabajo, o la computadora misma, impidiendo su uso normal por parte del usuario.

Acción Penal. Es la exteriorización de la voluntad indispensable para la actuación del Derecho penal objetivo. Es, por tanto, la base y la razón de ser del proceso penal, haciendo legitimo su normal desenvolvimiento.

Acción Pública. La acción penal, salvo los casos expresamente determinados por la ley, debe iniciarse de oficio, ejercitada obviamente por el ministerio público, sin perjuicio del Derecho de acusar o de intervenir como parte querellante en el juicio.

Acto Preparatorio del Delito. La actividad criminal comienza con actos previos que, en sí, no son punibles.

Acusación. Es la acción del representante del Ministerio Público o de personas con que se pide al juez penal que castigue el delito cometido por el acusado.

Adware. El adware es el software que utilizan los programas de spyware, que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla. Esta práctica se utiliza para subvencionar económicamente la aplicación, permitiendo que el usuario la obtenga por un precio más bajo e incluso gratis y, por supuesto, puede proporcionar al programador un beneficio, que ayuda a motivarlo para escribir, mantener y actualizar un programa valioso. Algunos programas adwares son también

shareware, y en estos los usuarios tiene la opción de pagar por una versión registrada o con licencia, que normalmente elimina los anuncios.

Agraviado. El damnificado por el delito. Es la víctima de una ofensa o perjuicio que se ha irrogado a sus derechos e intereses.

Ataques de autenticación. Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

Bomba lógica. Es una parte de código, insertada en un programa informático intencionadamente que permanece oculto hasta cumplirse una o más condiciones pre programadas, en ese momento se ejecuta una acción maliciosa.

Ciberespacio. El auge de las comunicaciones entre ordenadores, cuyo máximo exponente es la macrored mundial Internet, ha creado un nuevo espacio virtual, poblado por millones de datos, en el que se puede "navegar" infinitamente en busca de información. Se trata, en una contracción de cibernética y espacio, del ciberespacio.

Caballos de Troya. Programas que introducen conjunto de instrucciones no autorizadas. Consiste en introducir en un sistema conocido por el autor de la maniobra y desconocido por la víctima, un programa a través del cual el autor puede acceder a ese u otros programas del usuario.

Causa criminal. Es el expediente que se inicia con la presentación de la denuncia ante las autoridades, competentes, hasta el nivel de pronunciamiento de la sentencia y el fallo del más alto nivel del tribunal.

Código de acceso. Información o contraseña que autentica a un usuario autorizado en un sistema de información, que le permite el acceso privado y protegido ha dicho sistema.

Código de identificación. Información, clave o mecanismo similar, que identifica a un usuario autorizado en un sistema de información.

Código malicioso. Todo programa, documento, mensaje y/o secuencia de cualquiera de estos, en un lenguaje de programación cualquiera, que es activado induciendo al usuario quien ejecuta el programa de forma involuntaria y que es susceptible de causar algún tipo de perjuicio por medio de las instrucciones con las que fue programado, sin el permiso ni el conocimiento del usuario.

Copiado de fuentes. Consiste en que empleados de una empresa obtienen una copia de un determinado software hecho a medida de ésta, lo modifican y lo venden como si fuera un desarrollo propio.

Clonación. Duplicación o reproducción exacta de una serie electrónica, un número o sistema de información, que le permite el acceso privado y protegido ha dicho sistema.

Delito. Culpa, crimen, violación o quebrantamiento de la ley. Acción u omisión voluntaria, que la ley castiga con pena grave.

Delito de alta tecnología. Aquellas conductas atentatorias a los bienes jurídicos, protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones.

Firma electrónica. Datos cifrados de tal manera que el receptor pueda comprobar la identidad del transmisor.

Hackers. Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el Fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes. Experto que puede conseguir da un sistema informático cosas que sus creadores no imaginan.

Informática. Ciencia que estudia el tratamiento automático y racional de la información, a través de los ordenadores. Este término se refiere a lo mismo que computación, solo que informática tiene origen francés y computación origen inglés.

Información. Tras la revolución industrial, se habla de la revolución de la información, que se ha convertido en el mayor valor de las empresas y de las personas. El auge, proliferación y universalización de sistemas de interconexión global como Internet, ha llevado a hablar de la sociedad de la información como el nuevo paradigma del mundo en que vivimos.

Internet. Conjunto de redes de ordenadores creada a partir de redes de menos tamaño, cuyo origen reside en la cooperación de dos universidades estadounidenses. Es la red global compuesta de limes de redes de área local y de redes de área extensa que utiliza un protocolo para proporcionar comunicaciones de ámbito mundial a hogares, negocios, escuelas y gobiernos.

Microforma. Es una figura jurídica con un alto componente informático, creada en el Perú para que las imágenes de los documentos digitalizados tengan el mismo valor probatorio que un documento en papel.

Passwords. Es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. Aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

Pharming. Es una variante de Phishing, pero más sofisticada. A través de esta acción, los ladrones de datos consiguen que las páginas visitadas no se correspondan con las auténticas, sino con otras creadas para recabar datos confidenciales, sobre todo relacionadas con la banca online. El internauta introducirá sus datos confidenciales sin ningún temor, sin saber que los está remitiendo a un delincuente.

Phishing. Los phishers simulan pertenecer a entidades bancarias de reconocido prestigio y solicitan a los cibernavegantes datos de tarjetas de crédito o claves bancarias, a través de un formulario o un correo electrónico con un enlace que conduzca a una falsa página web, con una apariencia similar a la de la web original. En este caso, es el propio incauto internauta quien proporciona los datos requeridos, permitiendo al autor del ilícito lograr un beneficio económico ilegitimo.

Piratería de Software. Es en principio el copiado y la utilización no autorizada de programas protegidos por las leyes de copia o fuera de lo establecido en el contrato de licencia del mismo. Esto puede tener como agravante la venta del software a terceros. Puede efectuarse sobre textos, fotografías, y ahora aún el diseño de las páginas Web.

Prehacking. Es la utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio.

Programas. Es un conjunto de instrucciones que una vez ejecutadas realizarán una o varias tareas en una computadora. Sin programas, estas máquinas no pueden funcionar correctamente. Al conjunto general de programas, se le denomina software y así, se refiere al equipamiento lógico o soporte lógico de una computadora digital.

Red informática. Interconexión entre dos o más sistemas informáticos o entre sistemas informáticos y terminales remotas, incluyendo la comunicación por microondas medios ópticos, electrónicos o cualquier otro medio de comunicación, que permite el intercambio de archivos, transacciones y datos, con el fin de atender las necesidades de información y procesamiento de datos de una comunidad, organización o un particular.

Seguridad. Calidad de seguro. Condición de ciertos mecanismos que aseguran el buen funcionamiento de alguna cosa.

Sistema de información. Dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como cualquier sistema de alta tecnología, incluyendo, pero no limitado a los sistemas electrónicos, informáticos, de telecomunicaciones y telemáticos, que separado o conjuntamente sirvan para generar, enviar, recibir, archivar o procesar información, documentos digitales, mensajes de datos, entre otros.

Sistema electrónico. Dispositivo o conjunto de dispositivos que utilizan los electrones en diversos medios bajo la acción de campos eléctricos y magnéticos, como semiconductores o transistores.

Sistema informático. Dispositivo o conjunto de dispositivos relacionados, conectados o no, que incluyen computadoras u otros componentes como mecanismos de entrada, salida, transferencia y almacenaje, además de circuitos de comunicación de datos y sistemas operativos, programas y datos para el procesamiento y transmisión automatizada de datos.

Snooping. Obtener información sin modificarla **por** curiosidad y también con fines de espionaje o de robo.

Spam. Son mensajes electrónicos (habitualmente de tipo comercial) no solicitados y en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de internet que han sido objeto de spam incluyen mensajes, grupos de noticias usenet, motores de búsqueda y blogs. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.

Spoofing. Técnica para conseguir el nombre o password de un usuario legítimo, una vez que se ingresa al sistema consiguiendo este nombre se puede cometer cualquier tipo de actos irregulares en nombre del legítimo usuario. Ejemplo envío de falsos e-mails.

Spyware. Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos

programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos. Persona física o jurídica que adquiere de manera, legitima bienes o servicios de otra.

Sujeto activo. Es aquel que intencionalmente viole o intente violar, por acción, omisión o por mandato cualquiera las actuaciones descritas en la Ley.

Sujeto pasivo. Es aquel que se sienta afectado o amenazado en cualquiera de sus derechos por la violación de las disposiciones previstas en la Ley.

Tecnología. Conjunto de los conocimientos propios de las ciencias. Tratado de los términos técnicos.

2.2. Bases teóricas

2.2.1. Delitos informáticos

Sobre el significado de delito informático se anotan tres definiciones de gran valor:

- Es cualquier acción ilegal en la que el ordenador sea el instrumento o el objeto del delito y, más concretamente, cualquier delito ligado al tratamiento automático concretamente de datos;
- Cualquier acto criminoso relacionado con la tecnología informática, por el cual una víctima ha sufrido una pérdida y un autor ha obtenido intencionalmente una ganancia.
- Cualquier conducta ilegal, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos.

2.2.2. Bases teóricas especializadas sobre el tema.

2.2.2.1. Concepto de informática. La informática constituye un fenómeno-ciencia que ha logrado penetrar en todos los ámbitos o áreas del conocimiento humano, y siendo el Derecho una ciencia, por cuanto constituye un área del saber humano, reflejándose en un conjunto de conocimientos, pues, no cae en la excepción de ser tratada por la informática,

dando lugar en términos instrumentales a la Informática jurídica, que consiste en una ciencia que forma parte de la Informática, que al ser aplicada sobre el Derecho busca el tratamiento lógico y automático de la información legal. Podemos denominar al concepto de informática como la ciencia que estudia los ordenadores. El concepto de informática viene dado de la unión de dos palabras Información y automática. En inglés se habla de conceptos tales como Computer Science, Electronic Data Processing, etc.

Según Núñez (1996) "es el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores" (p. 19).

Abordando el concepto de informática según el diccionario académico de la Lengua Española, se le puede definir como aquella ciencia encargada de estudiar los ordenadores y su capacidad para procesar y almacenar información y datos. Las funciones principales de la informática son las siguientes:

- Creación de nuevas computadoras.
- Creación de nuevas especificaciones de trabajo.
- Desarrollo e implementación de sistemas informáticos.
- Optimización de los métodos y sistemas informáticos existentes.
- La informática es aplicada en diversos sectores de la actividad diaria".

En sus inicios, la informática facilitó los trabajos repetitivos y monótonos del área administrativa, gracias a la automatización de esos procesos, lo que a su vez trajo como ventaja una disminución de los costes. Dentro del concepto de informática, su principal función es facilitar información oportuna y veraz, lo cual facilita la toma de decisiones a nivel empresarial

2.2.2.2. Desarrollo de la informática. El avance de la informática en el mundo actual, es de tal magnitud que se ha llegado a sostener que se constituye en una forma de Poder Social. Las facultades que el fenómeno informático pone o coloca a disposición de los gobiernos y de las personas naturales o jurídicas, con rapidez y ahorro consiguiente de tiempo

y energía, configuran un panorama de realidades de aplicación y de posibilidades de juegos lícitos e ilícitos, en donde resulta necesario e imprescindible el derecho para regular los múltiples efectos de una situación nueva y de tantas potencialidades en el medio social.

En efecto, actualmente no solo se usa las computadoras como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medios eficaces para obtener y conseguir información privilegiada, constituyendo de ese modo un nuevo medio de comunicación. Asimismo, condiciona el desarrollo de la informática, la misma que en esencia se resume en la creación procesamiento, almacenamiento y transmisión de datos.

La informática está presente en todas las actividades más o menos importantes que desarrolla el hombre en la vida moderna. Todas las ramas del saber humano se rinden ante los progresos tecnológicos y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos se hacían manualmente. No obstante, el desarrollo sostenido de la informática también ha dado paso a conductas antisociales y delictivas que se manifiesta de formas que eran imaginables en tiempos pasados. Los sistemas de computadoras ofrecen oportunidades nuevas y complicadas de infringir la ley, creando de esa forma la posibilidad de cometer delitos tradicionales en formas no tradicionales.

El desarrollo de la informática ha ocasionado la aparición de nuevos delincuentes, quienes haciendo uso de los conocimientos de la informática obtienen ingentes beneficios económicos indebidos en perjuicio evidente de otros. Ante tal panorama, el legislador comenzó a preocuparse y formular políticas criminales de acción para hacer frente a los que muy bien podemos denominar “delincuentes informáticos” y otros denominan delincuentes de cuello blanco.

2.2.2.3. La delincuencia informática. Para graficar la situación en la cual se encuentra el mundo respecto de los delitos informáticos, se puede tener como referencia en torno al ejemplo casuístico de la sentencia dada el 20 de febrero del 2002, en que el Tribunal

de Gran Instancia de Lyon – Francia condenó a la pena de ocho meses de prisión y multa a quien alteró el funcionamiento de los sistemas de procesamiento automatizado de datos de una sociedad. El autor había ingresado en forma fraudulenta en el sistema de procesamiento de datos y remitió, mediante la utilización de un programa, gran cantidad de correos electrónicos infectados con el virus informático y sendos archivos que provocaron distintos desperfectos en el uso de los sistemas de los ordenadores personales.

En el Perú el legislador del Código Penal de 1991 pretendió hacer frente al problema desde una visión patrimonialista, incorporando delitos que estén acordes con las nuevas formas de criminalidad informática. En efecto, el legislador peruano considerando que con las acciones de los delincuentes informáticos se afectaba el bien jurídico patrimonio de la víctima, en el inciso tres del artículo 186 del C.P., reguló como agravante el uso de los conocimientos y máquinas de la informática. Este dispositivo prevé que se configura el delito de hurto agravado cuando el agente actúa mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general o la violación del empleo de claves secretas.

Como antecedente se contempló en el Código Penal Peruano en base a lo que se dio por parte de la Ley N° 27309 del 2000, se reguló tres supuestos que en doctrina desatinadamente se conocen como delitos informáticos. Por tal razón ya afirmaba Bramont Arias Torres que con los delitos informáticos, en realidad no se protegía ningún bien jurídico, porque en verdad no hay, como tal un delito informático. Este no es más que una forma o método de ejecución de conductas delictivas que afectan a bienes jurídicos que ya gozan de una específica protección por el derecho penal.

Esa postura asumió el legislador y optó por introducir a los mal llamados delitos informáticos como modalidades de comisión de conductas delictivas ya tipificadas. De ese modo, encontramos reunidas tres circunstancias que agravan la figura delictiva del hurto; primero, cuando la sustracción se realiza mediante la utilización de sistemas de transferencia

electrónica de fondos; segundo, cuando el hurto se efectúa por la utilización de la telemática en general; y, tercero, cuando el hurto se produce violando claves secretas. Estas circunstancias agravantes tienen naturaleza de materialización distinta aun cuando la finalidad sea la misma: obtener provecho económico indebido por parte del agente en perjuicio de la víctima.

En forma breve, transferir electrónicamente fondos es trasladar, movilizar, desplazar dinero de una cuenta a otras sin recibos, firmas ni entregas materiales y sobre todo, sin remitir o enviar físicamente el dinero. El segundo supuesto se configura cuando el agente haciendo uso de la telemática que viene a constituir el tratamiento de información a distancia haciendo uso de las telecomunicaciones asociadas a la informática (el Internet, comercio electrónico), sustrae en forma ilícita bienes valorados económicamente en su beneficio.

En tanto que el último supuesto se configura cuando el agente haciendo mal uso o, mejor dicho, mal empleo de las claves secretas que sabe o conoce porque le han sido confiadas por su titular, comete el hurto. Si llega a determinarse que el sujeto activo no tenía las claves secretas y más bien entró en conocimiento de ellas haciendo uso de la informática o por otros medios, no se verifica la agravante, subsumiéndose tal conducta en las otras circunstancias ya comentadas, pues en aquellas necesariamente se viola claves secretas con las cuales se encuentran protegidas las operaciones del ciberespacio.

Sin embargo, no pasó mucho tiempo para darse cuenta el legislador peruano que lo previsto en el inciso 3 del artículo 186 del Código Penal de 1991, solo servía para sancionar a un reducido grupo de conductas patrimoniales, dejando sin sanción punitiva gran número de conductas dañosas, es decir, no servía para hacer frente a los típicos delitos informáticos que sin duda causan perjuicio enorme a los intereses patrimoniales de los propietarios de las máquinas u ordenadores y redes informáticos. Aquellas figuras delictivas de carácter patrimonial no servían para reprimir la manipulación fraudulenta de los ordenadores con ánimo

de lucro, la destrucción de programas o datos y el acceso y utilización indebida de la información que puede afectar la privacidad de las personas tanto naturales como jurídicas.

Conductas con las cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no solo la cuantía de los perjuicios así ocasionados es superior a la que es usual en la delincuencia tradicional, sino también, son mucho más elevadas las posibilidades que no llegue a descubrirse los hechos ilícitos. Los delincuentes informáticos son especialistas capaces de borrar toda huella de sus hechos ilícitos. Sin duda, los conocimientos de la informática facilitan que la realización de la conducta prohibida no deje huella o pistas.

De tal modo las epidemias informáticas causadas por virus que destruyen a su paso archivos de todo tipo, páginas web peruanas que son desde hace varios años blanco de ataques perpetrados por hackers peruanos y extranjeros, la vulneración de sistemas informáticos por personas que ingresan indebidamente, la sustracción de información almacenada, etc., originaron que nuestro legislador haya optado por la tipificación de estas conductas delictuales, dictándose la Ley correspondiente. En nuestra patria, el 17 de julio de 2000, se promulgó la Ley Nº 27309 que incorpora los típicos delitos informáticos a nuestro Código Penal. Los mismos que en doctrina también se les conoce con las denominaciones de delitos electrónicos, delitos relacionados con la computadora, crímenes por computadora, delitos de cuello blanco o delitos relacionados con el ordenador.

El delito informático o electrónico puede ser definido como aquella conducta típica, antijurídica, culpable y punible en la que la computadora, sus técnicas y funciones desempeñan un papel trascendente, ya sea como método, medio o fin en el logro de los objetivos indebidos del agente, cual es el logro de algún perjuicio de tipo patrimonial a su víctima. En términos más sencillos también se le puede definir como toda conducta típica, antijurídica, culpable y punible en la que el agente hace uso de cualquier medio informático para obtener un beneficio

en perjuicio del sujeto pasivo. Expuestos así los planteamientos centrales, puede inferirse que las conductas efectuadas por medio de la informática no protegen un derecho patrimonial expresado funcionalmente en el sistema económico, sino un nuevo bien jurídico desarrollado por la tecnología informática y que puede tener tanto una aplicación económica como también doméstica. En este sentido puede concluirse que tampoco estos delitos patrimoniales forman parte del derecho penal Económico

2.2.3. Los cambios sociales producto de la informática.

No cabe duda que la época actual es una era de la informática. De ahí que expresiones como la sociedad de la información y similares son muy utilizados en la doctrina cuando se aborda la problemática de los delitos informáticos ha permitido en un mundo de posguerra fría, y era de la globalización, mayores contactos entre civilizaciones, cuando antes eran Intermitentes o inexistentes:

La arremetida de la informática ha dado nacimiento a lo que Naipul llamó una civilización universal. ¿Qué significa esa expresión? La idea implica, en general, la confluencia de la humanidad y la creciente aceptación de valores, creencias, orientaciones, prácticas e instituciones comunes por pruebas y personas de todo el mundo (Huntington, 1997). Así en los actuales tiempos es posible que en tiempo real y casi de inmediato una persona se comunique con otra en otro lado del mundo mediante una computadora. Sectores como la banca, los seguros, los transportes, la educación, la bolsa, el tráfico aéreo y terrestre, las Administraciones Públicas dependen en gran medida, de las computadoras.

La bifurcación cultural producto de la informática es cada vez menor. Hoy no es posible concebir una sociedad que no se encuentre marcado por la intromisión de la informática. Ello ha motivado incluso, el nacimiento de las civilizaciones globales, es decir, que ninguna sociedad puede ser entendida sin hacer referencia al entorno donde se ubica. La informática ha invadido todo tipo de negocios y empresas desde pequeñas hasta las más grandes. A ello ha

favorecido la masificación de las computadoras que ha llevado a una disminución de precios y la consecuente adquisición ser partes de sectores menos favorecidos.

Según Pérez (1987):

> La alta tecnología, en cuyas, redes se desenvuelve el vivir humano ordinario, nos ha preparado desde la infancia con una sucesión de inventos antes insospechados, y casi hemos perdido nuestra capacidad de asombro frente a lo que había tildado de sobrenatural en épocas precedentes" (p. 13).

El desarrollo científico y tecnológico coloca a la razón humana en condiciones de enseñorearse del mundo natural, pero, como en contraposición, corre el riesgo de ser absorbida por la racionalidad tecnológica. El riesgo, para este autor, reside en la pretensión de convertir la lógica del desarrollo tecnológico en principio supremo del vivir social.

A través de la informática, los cambios sociales son notorios y se habla ya de una mixtura social. El avance tecnológico ha permitido que los seres humanos, compartan valores básicos como valoraciones negativas sobre determinados hechos. La totalidad de las instituciones dedicadas al comercio tienen necesidad de la informática. La alta tecnología en el campo de la informática ha cambiado algunos patrones y hábitos culturales. Las novedades culturales se han difundido de manera rápida y eficaz mediante el uso de las computadoras. En igual sentido, políticas culturales de expansión como de consumo se hacen a través de informática. Las innovaciones eliminan poco a poco los inconvenientes para el acceso al uso del internet. Los nuevos programas, buscan solucionar justamente inconvenientes al respecto.

De lo hasta aquí acotado se aprecia que la delincuencia informática es de reciente cuño. Por ello es que su regulación jurídica es de creciente data. Así en nuestro país los delitos informáticos no fueron previstos en el C.P. de 1991, siendo introducción recién mediante Ley N° 27309 del 17 de Julio del 2000, modificando el Título V del Libro Segundo del Código Penal. También es bueno recalcar que el fenómeno de la criminalidad vinculada a la

informática no lleva necesariamente el sello de las grandes potencias, sino que se presenta, como señala Tiedemann (1985), "con las lógicas diferencias de matiz, en toda comunidad donde se incorporan computadoras con independencia de la conformación de los sistemas económicos" (p. 121).

Así cada país ha venido y viene enfrentando esta problemática desde su experiencia y desde su óptica al respecto, aunque la experiencia jurisprudencial es inexistente hasta ahora. Esto debido a la poca implementación de medios eficaces para su detección. La sociedad peruana, no ha quedado como puede corroborarse alejada de este proceso de revolución en la informática. Incluso algunas consultas y operaciones en materia tributaria se hacen mediante el uso de la informática.

Dialécticamente se puede entender la criminalidad informática como aquella negación o contradicción que conlleve todo fenómeno, como lo es: La revolución de la comunicación mediante la informática. Por lo demás, no puede negarse el carácter global del fenómeno informático y consecuentemente el de su criminalidad propiciada por el ordenador. Su incidencia en la economía y la seguridad de un país, es superar al de otras manifestaciones de criminalidad, así como su magnitud en el ámbito que la afecta, de ahí que no obstante su inexistencia típica en el CP, de 1991, el legislador haya tenido que incluirse en el sistema penal.

2.2.4. Valoración social de la informática.

Desde otro punto de vista, para García (1984) "la informática se presenta como una nueva forma de poder" (p. 39), que puede estar concentrado en un grupo privado de poder o como monopolio estatal. Su uso puede no sólo facilitar el desarrollo humano sino además porque ella significa el nacimiento de una nueva forma de comunicación, que ha influido cualitativamente en la naturaleza humana. Así el analfabeto del siglo XXI será quien no sepa usar una computadora.

La informática marca hoy la frontera entre las sociedades modernas. En tal sentido, como señala Frosini (1982), la informática es "factor de conocimiento y de poder" (p. 173), que puede ser concebido como nuevo tejido cohesionador de la sociedad civil o como un instrumento de sumisión universal. Sin embargo, existen voces que cuestionan la intromisión de la tecnología en el desarrollo social, con la que se bosqueja una sociedad alienada, sometida a aparatos cada vez más sofisticados de control social e integrada por una masa despersonalizada de individuos, cuyas características distintivas serían el aislamiento, el extrañamiento y la pasividad.

No puede compartirse las expresiones antes acotadas pues la informática a no dudarlo ha significado un cambio en el concepto de alfabetización. Estos cambios en alfabetización, educación y urbanización crearon poblaciones socialmente con mayores capacidades y expectativas más elevadas, susceptibles de nuevas formas de movilización con fines políticos, inaplicables a los campesinos alfabetos. Una Sociedad movilizada socialmente es una sociedad más poderosa. Desde nuestra limitada perspectiva, no podemos entrar en profundidad a valorar la repercusión global de la revolución informática (de lo que se ocupan filósofos, sociológicos y economistas y que desbordarían el propósito del presente trabajo).

Baste apuntar, no obstante, como sostiene Gutiérrez (1991) "que tan evidente resulta a los ojos del observador su dimensión de progreso como la de riesgo" (p. 87). Con toda seguridad, no estamos en la sociedad ideal referente a una sociedad con alta creatividad intelectual, en la que la gente pueda diseñar intenciones futuras sobre un lienzo invisible y perseguir y conseguir su autorrealización. No importa la opinión que se tenga sobre las ventajas o perjuicios del avance tecnológico referente a la informática, no puede negar lo que es una realidad: la informática ha elevado la calidad humana cuya irreversibilidad es incuestionable. La informática está entre nosotros y paredes que permanecerá en ella en el futuro.

2.2.5. Informática y derecho penal.

No cabe duda de que la aparición de nuevas tecnologías en el ámbito del Derecho y del Derecho Penal en especial. Frente a ello se debate de si los mecanismos jurídicos son los adecuados para frenar las conductas no deseadas que siempre traen las nuevas tecnologías, sobre todo en lo referente al beneficio económico y a la forma de obtenerlo. El Derecho penal no debe ser manipulado como un medio totalmente independiente de los restantes recursos y procesos que conforman el arsenal del "control social" estatal. Constituyendo así una parte de la política social general, y encontrándose en las relaciones y condiciones sociales las causas de las acciones delictuosas, la lucha contra ellas debe realizarse, en primera línea, no mediante la pena sino con intervenciones sobre dichos factores sociales.

Respecto a este carácter secundario del derecho penal, Maurach citado por Hurtado (1987) sostiene que no se trata sino de una exigencia ética planteada al legislador. De ahí que el Derecho penal sólo debe intervenir en aquellos actos que atenten gravemente contra bienes jurídicos protegidos. Su intervención debe ser útil; de lo contrario pierde su justificación (Bramont, 1997).

De acuerdo a lo indicado por Mir (1990): "Cuando se demuestre que una determinada reacción penal es inútil para cumplir su objetivo protector, deberá desaparecer, aunque sea para dejar lugar a otra reacción penal más leve" (p. 98).

A título de ejemplo, considérense los problemas que se crean en el área de los derechos de autor en relación con los programas -, el tema de la información como objeto del Derecho, la incidencia de la informática en el tráfico bancario y empresarial, la utilización de las nuevas técnicas respecto a la prueba procesal. Se comprende sin dificultad que la conmoción que la informática provoca sobre el ordenamiento es de extraordinaria magnitud, pues son múltiples las disciplinas afectadas de forma directa: el Derecho Civil, el Derecho mercantil, la Parcela Tributaria, la procesal, e indudablemente, la penal.

Teniendo en cuenta que la intervención del Derecho penal es de por sí por causas extremas (ultima ratio), nos lleva a que las causas para su intervención en materia de informática sean por la utilización indebida de técnicas con consecuencias graves para terceras personas que, claro, puedan ser constatables objetivamente. De ahí que uno de los problemas que presenta la lucha contra los delitos informáticos sea el que se da en el ámbito procesal. Pues lo que suele suceder es que sea fácil probar el perjuicio no así, identificar al autor, ni el lugar de done lo hizo.

De ahí que le asiste razón que García (1988), cuando afirma que la informática ofrece un inmenso abanico de técnicas y estrategias que, eventualmente, pueden ponerse al servicio del crimen, enriqueciendo el repertorio criminal. Abre nuevos horizontes al delincuente, incita su imaginación, favorece su impunidad y potencia los efectos del delito convencional. Cada una de las notas con las que se presentan las nuevas tecnologías de la información en el entramado social y económico, ofrece su dimensión negativa (vulnerable). Son los riesgos de la informática, en virtud de los cuales esta puede adquirir, en su caso, relevancia jurídico-penal.

El primer punto de esta problemática tiene que ver con la información que se maneja a través de esta nueva tecnología. Esta información al ser muchas veces secreta, por su calidad, y al estar en un medio de fácil acceso, como es la informática, potencia su criminalidad. En este sentido la "información" significa en esta realidad virtual "poder". A mayor información, mayor poder, porque mediante ella se aumenta la capacidad de control de quien lo ostenta.

Paradójicamente a los beneficios de la informática, su perjuicio es notorio, pues mediante ello los individuos pierden parte de su libertad, pues su intimidad pende de la habilidad que pueda tener una persona para vulnerar su código de seguridad y acceder a su correspondencia virtual. Es conocido que una persona con mediana formación en informática puede ingresar indebidamente a un correo electrónico. En consecuencia, la sociedad moderna como el comercio está supeditado a este control informático.

En segundo lugar, no es desconocido que la información se ha convertido, en los últimos tiempos un bien un valor en el tráfico jurídico. Este valor en el mercado lo han convertido en un bien muy preciado, cuyo acceso clandestino está bien remunerado en el mercado negro. No es extraño el aceptar que la mayoría de la información industrial se almacena, procesa y transmite por medio de la informática. Así mismo muchos sistemas de seguridad están supeditados a la inaccesibilidad de su sistema informático.

No olvidemos tampoco, la dimensión instrumental de la informática que a la vez, llega a abrir infinitas posibilidades de progreso y desarrollo a la humanidad, pone a disposición de la inteligencia del delincuente un enorme abanico de vías para alcanzar su propósito criminal, dando a luz perspectivas nuevas de la delincuencia tradicional. En consecuencia, los tipos tradicionales, no bastan para abarcar, las nuevas modalidades delictivas emergentes del desarrollo de la sociedad producto del avance tecnológico, sobre todo porque estas presentan cualidades hasta ahora desconocidas.

Los fenómenos económicos de la globalización y de la integración económica dan lugar a la conformación de modalidades nuevas de delitos clásicos, así como la aparición de nuevas formas delictivas. Así, la integración genera una delincuencia contra los intereses financieros de la comunidad producto de la integración (fraude al presupuesto-criminalidad arancelaria-fraude de subvenciones), al mismo tiempo que contempla la corrupción de funcionarios de las instituciones de la integración. Por lo demás, generan la aparición de una nueva concepción de lo delictivo, centrada en elementos tradicionalmente ajenos a la idea de delincuencia como fenómeno marginal; en particular, los elementos de organización, transnacionalidad y poder económico. Para Silva (1999): “Criminalidad organizada, criminalidad internacional y criminalidad de los poderosos son, probablemente, las expresiones que mejor definen los rasgos generales de la delincuencia de la globalización” (p. 70).

2.2.6. Delitos informáticos - concepto

A nivel internacional no existe una definición propia del delito informático, pero se han formulado algunos conceptos en mérito a la realidad de los países afectados. Así, hasta antes de la promulgación de la mencionada ley, el Código Penal Peruano hacía alusión a una modalidad de hurto agravado, tipificado en el Art. 186, que podía catalogarse como una figura de delito informático, configurado cuando el hurto se cometía mediante la utilización de sistemas de transferencia electrónica de fondos; de la telemática, en general; o, se violaban claves secretas. El Código Penal Peruano, al incorporar la figura del delito informático, no establece una definición genérica del mismo, ergo, lo conceptualiza en forma típica como: las conductas típicas, antijurídicas y culpables, en que se tiene a las computadoras como instrumento o fin; y, atípica, entendiendo que los delitos informáticos son las actitudes ilícitas en que se tiene a las computadoras como instrumento o fin.

Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor, aunque no perjudique de forma directa o indirecta a la víctima, tipificado por La Ley, que se realiza en el entorno informático y está sancionado con una pena. De esta manera, el autor Téllez (1996) señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)" (p. 26).

Por otra parte, Callegari (1985) define al delito informático como “aquel que se da con la ayuda de la informática o de técnicas anexas”. El italiano Carlos Sarzana lo determina como “cualquier comportamiento criminógeno en el que la computadora está involucrada como material, objeto o mero símbolo”. De otro lado, Fernández (1996) lo describe como la realización de una acción que, reuniendo las características que delimitan el concepto de delito,

se ha llevado a cabo utilizando el elemento informático o telemático contra los derechos y libertades de los ciudadanos. Asimismo, el Departamento de Investigación de la Universidad de México califica de delitos informáticos a todas aquellas conductas ilícitas, susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático.

Castillo y Ramallo (1989) entienden que "delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas". Por su parte, Lilli y Massa afirman que la locución "delito informático" puede entenderse en un sentido restringido y otro amplio. En su concepto restringido, comprende los hechos en que se atacan elementos puramente informáticos (independientemente del perjuicio que pueda causarse a otros bienes jurídicamente tutelados y que eventualmente puedan concurrir en forma real o ideal); mientras que en su concepto amplio abarca toda acción típicamente antijurídica y culpable para cuya consumación se utilizó o se afecta una computadora o sus accesorios.

Estas definiciones deben ser precisadas para no inducir a error, ya que no todo ilícito en el que se emplee un computador como medio o instrumento para su consumación tendrá tal carácter, ya que puede tratarse de una figura típica tradicional informatizada a la que se llama delito computacional. Eso sí, se debe aclarar que no puede afirmarse que todo delito en el que interviene un computador como medio es un delito informático o un delito computacional, pues el uso que se le dé, debe ser el normal de acuerdo a su naturaleza. Por ejemplo, no sería un delito computacional las lesiones que se le causen a una persona golpeándolo con un monitor o un teclado, por ejemplo. Por lo tanto, una primera conclusión que nos llevará a un concepto de delito informático es excluir de la definición a los delitos computacionales.

Ahora bien, teniendo claro que se busca conceptualizar las conductas ilícitas nuevas, cometidas generalmente a través de equipos computacionales, pero en donde el elemento central no es el medio de comisión, sino que es el hecho de atentar contra un bien informático,

se hace necesario destacar que no todos los bienes informáticos son objeto de estos delitos. Los sistemas de tratamiento automatizado de la información se basan en dos grandes tipos de soportes, el físico y el lógico. Así, por una parte, como señala Riquert (2014), "los bienes informáticos que vienen a ser el soporte físico conforman el hardware, es decir, los equipos computacionales, que son bienes corporales muebles como el procesador o la unidad central de proceso y los dispositivos periféricos de entrada y salida, como, por ejemplo, el monitor, el teclado, la impresora, un escáner, etc." (p. 2).

En cambio, por la otra, existen bienes intangibles que constituyen el soporte lógico del sistema o software. Dentro de él están los datos digitalizados (es decir, transformados a un lenguaje computacional basado en un sistema binario o de base 2, en donde sólo existen dos cifras, los ceros y los unos), que se ingresan al computador para que sean procesados y puedan constituir información. Además, se encuentran otros bienes informáticos como los programas computacionales, que son un conjunto de instrucciones para ser usadas directa o indirectamente en un computador a fin de efectuar u obtener un determinado proceso o resultado. Pues bien, no todos los bienes computacionales son objeto de delitos informáticos. Contra el hardware o soporte físico se cometen delitos convencionales o delitos computacionales (si usa como instrumento a la computación), pero no delitos informáticos, es decir, figuras nuevas no encuadrables en las ya existentes.

Si los equipos computacionales son bienes tangibles, corporales, muebles no hay inconvenientes para que se cometan en su contra los tradicionales delitos de hurto, robo o daños. De esta forma, descartamos la incorrecta idea que algunos autores sostienen en relación a calificar como delitos informáticos al hurto de un computador, el robo de un cajero automático, los incendios intencionales y atentados terroristas en contra de una central de computación, por ejemplo. Es más, incluso empleando como medio de comisión a las

tecnologías de la información no estamos en presencia de un delito informático, sino que, en ese caso, de un delito computacional.

Por ejemplo, el introducir un virus físico o destructivo, que altera el funcionamiento del sistema exigiéndolo más allá de sus capacidades logrando un sobrecalentamiento que acarrea que se queme, por ejemplo, el disco duro, la tarjeta de video o el monitor, es un delito de daños convencional informatizado o delito computacional. Hay autores que clasifican estas conductas destinadas a destruir los elementos físicos del sistema dentro del sabotaje informático. Ellos justifican la penalización de tales conductas como delitos informáticos basados en la desproporción que existe entre el valor de los equipos y el perjuicio que implica la destrucción correlativa; en la impunidad de los autores favorecida por la detectabilidad del ilícito bastante tiempo después; y por la gran dificultad que presentan para valorar la real cuantía del daño producido en atención al valor del material destruido.

Por lo tanto, la definición que considero más apropiada para los delitos informáticos es toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable, y atente contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del empleo de las tecnologías de la información, y el cual se distingue de los delitos computacionales o tradicionales informatizados. Esta idea es compartida por el autor más prestigioso de Europa en relación a los delitos informáticos, el profesor alemán Sieber, quien los define como todas las lesiones dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente.

De la definición aclarará para terminar este punto, que no todos los datos digitalizados merecen una protección penal (sí una protección civil o administrativa frente al mal uso que se les dé). Sólo los datos relevantes deben ser protegidos penalmente. Por ejemplo, en relación a los datos personales, sólo los datos sensibles deben protegerse creando delitos, es decir, aquellos datos que son muy personales y que permiten llegar a conformar un perfil del

individuo que puede ser usado para discriminarlo, como su tendencia política, religiosa, sexual, historial, médico, etc.

2.2.7. *Características*

De acuerdo con lo enunciado por el Dr. Téllez, en su libro intitulado 'Derecho Informático' se pueden destacar las siguientes características: Son conductas criminógenas de cuello blanco, en tanto que solo un determinado número de personas, en este caso ingenieros de sistemas o técnicos, pueden llegar a cometerlas.

- Son acciones ocupacionales, ya que generalmente se ejecutan cuando el sujeto se encuentra en pleno trabajo.
- Son acciones de oportunidad, en cuanto se aprovecha la ocasión presentada.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios de más de cinco cifras a quienes los realizan".
- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundos y sin una necesaria presencia física del ejecutante pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias debido a la falta o escasa regulación por parte del Derecho.
- Debido a su carácter técnico presentan grandes dificultades para su comprobación.

2.2.8. Clasificación

Los delitos informáticos han sido objeto de variadísimas clasificaciones, y se han tenido en cuanta a estos efectos:

- El perjuicio causado
- El papel que el computador desempeñe en la realización del mismo.
- El modo de actuar.
- El tipo penal en que se encuadren.
- Clase de actividad que implique según los datos involucrados.

Según Téllez clasifica a los delitos informáticos en base a dos criterios:

a) Como instrumento o medio:

Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

b) Como fin u objetivo:

Se enmarcan a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

María de la Luz Lima, clasifica los delitos electrónicos en tres categorías, de acuerdo a como utilizan la tecnología electrónica:

c) Como método:

Cuando los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

d) Como medio:

En donde para realizar un delito utilizan una computadora como medio o símbolo.

e) Como fin:

Conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

2.2.9. El bien jurídico tutelado

Con la promulgación de la última Ley Penal de Delitos Informáticos, ley punitiva con carácter especial, que se dio en el Perú, la Ley N° 30096 del 22 de octubre de 2013, que derogó a la anterior tipificación penal de tales ilícitos que se había contemplado dentro del Código Penal vigente; se tiene que con la mencionada Ley 30096, se ha contemplado una regulación penal amplia en nuestro país, de manera más completa, sistematizada y uniformizada de todos los ilícitos informáticos que se pueden llegar a perpetrar, subclasificándose la comisión de los delitos que se perpetran con el uso aplicativo indebido de los procedimientos, técnicas y tecnologías de informática, en aquellos que llegan a vulnerar la intimidad, honor, reputación y

privacidad personal de los ciudadanos que resultan afectados, sobre todo los personajes de índole público, que son vulnerados al difundirse indebidamente, y sin su autorización, imágenes como videos de su estricta privacidad, que resultan transmitidos ilegalmente por las redes sociales informáticas; y que asimismo se tiene en segundo orden clasificatorio, a los ilícitos informáticos que atentan contra el patrimonio económico de las personas, considerándose los casos de robos informáticos y estafas - electrónicas, que se perpetran mediante las modalidades de pishing y de empleo de virus informáticos para la perpetración de tales ilícitos, que llegan a cometerse por los ciberdelincuentes o hackers informáticos accediendo indebidamente sin permiso alguno, a las cuentas bancarias de los ciudadanos, de hacerse pasar como ellos o de engañarlos para obtener sus claves de acceso, y con ello de poder retirar ilícitamente todo el dinero de las cuentas bancarias que posean los usuarios afectados en las Entidades Bancarias; mientras que en tercer lugar se tienen a las modalidades ilícitas informáticas que perpetran los delincuentes hackers como el acceso indebido a información contenida en bases informáticas de datos, el de realizar actos ilegales de interceptación de datos informáticos, y entre otros delitos relacionados.

Asimismo, se tienen que los delitos económico-patrimoniales vinculados a la informática tratarían sobre ataques al bien jurídico patrimonio, realizados a través de la informática y siempre llevados a cabo con la "intención" de consumar apoderamientos o beneficios económicamente evaluables sobre el patrimonio de terceras personas (estafa informática y espionaje informático de secretos de empresa, por ejemplo). En relación con los atentados por medios informáticos contra la intimidad y la privacidad, cabe indicar que, para dicho sector de opinión, constituyen ataques al bien jurídico privacidad, pero como un concepto que incluyendo el de intimidad, va más allá, pues abarca todas las modalidades protegidas en el art. 18 CE [Constitución española] (el honor, la intimidad personal, la familiar, la propia

imagen, el domicilio, el secreto de las comunicaciones o el uso correcto de la informática) (Gálvez et al., 2011).

2.2.10. Caracterización de los sujetos.

2.2.10.1. Sujeto activo. No se está hablando de delincuentes comunes. Los sujetos activos tienen como características:

a) Poseen importantes conocimientos de informática.

b) Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible (se los ha denominado delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema).

c) A pesar de las características anteriores se debe tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

d) Las opiniones en cuanto a la tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional a nivel informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

e) Estos delitos se han calificado de "cuello blanco", porque el sujeto que comete el delito es una persona de cierto status socioeconómico.

La "cifra negra" es muy alta. No es fácil descubrirlo ni sancionarlo, en razón del poder económico de quienes los cometen y también es importante destacar que los daños económicos son altísimos. Se habla de pérdidas anuales por delitos informáticos y otros tecno-crímenes,

que van desde los U$S 100 millones (Cámara de Comercio de los Estados Unidos) hasta la suma de U$S 5.000 millones, de acuerdo a un estudio de 1990 hecho por una firma auditora.

Pacheco (s.f.) nos dice:

> Otro estudio estimó que sólo el 1% de los robos de computadora son detectados, y quizá sólo un 15 % de ellos sean denunciados. Cuando los delitos informáticos son denunciados y llevados a juicio, muchos de ellos son negociados fuera del juzgado; sólo alrededor del 24 % van realmente a juicio, y alrededor de dos tercios de esos juicios resultan en la absolución y el archivo del expediente (p. 76).

Un punto importante es que la opinión pública no considera delincuentes a estos sujetos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor de estos delitos distingue entre el daño a las personas (que es inmoral) y el daño a las organizaciones, porque en este último caso sienten que "hacen justicia", se le ha llamado a este punto de vista el síndrome de Robin Hood.

2.2.10.2. Sujeto pasivo. Es la persona o entidad sobre el cual recae la conducta que realiza el sujeto activo. la mayoría de los delitos informáticos no son descubiertos, como ya dijimos, pero es importante destacar que se debe en gran parte a que los mismos no son denunciados, las empresas o bancos tienen miedo al desprestigio y a su consecuente pérdida económica.

Vera (1996) sostiene que las características de las víctimas de los delitos son: Personas Jurídicas, Bancos, Compañías de Seguros Empresas públicas y privadas. No denuncian los delitos por temor a pérdida de imagen corporativa (Seriedad, solvencia y seguridad) Solución mediante medidas internas (despidos o aumentos de medidas de seguridad). Situación favorece a delincuentes (generalmente no se denuncian los delitos, se llega a un acuerdo con el delincuente).

Según Magliona (2003), las víctimas de estos delitos son generalmente personas jurídicas. Se trata, usualmente de bancos compañías de seguros, empresas públicas y privadas, sin importar si cuentan o no con medidas técnicas de protección. Una vez que estas asociaciones detectan las conductas ilícitas de las cuales han sido objeto, suelen no denunciar los delitos por temor a sufrir una pérdida de su imagen corporativa. No están dispuestas a perder la imagen de seriedad, solvencia y seguridad y antes de ver sus debilidades expuestas, prefieren solucionar sus problemas mediante la aplicación de medidas internas, como despidos o aumentos de seguridad. Por supuesto esa actitud no hace sino favorecer a los delincuentes, quienes continuaran con sus conductas con la mayor impunidad.

2.2.10.3. Tipos de delitos informáticos. Entre las diversas modalidades de delitos informáticos que se pueden presentar tenemos:

2.2.10.3.1. Fraudes cometidos mediante manipulación de computadoras. Según Levene y Chiavalloti (s.f.) indican que "Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas" (p. 51). Se clasifican en las siguientes modalidades delictivas:

2.2.10.3.2. Manipulación de los datos de entrada. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

2.2.10.3.3. Manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos y concretos de informática.

Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el

denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

2.2.10.3.4. Manipulación de los datos de salida. Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

Tradicionalmente como refiere Núñez (1996):

> Esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito (p. 75).

2.2.10.3.5. Fraude efectuado por manipulación informática. Se aprovechan las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2.2.10.3.6. Falsificaciones informáticas

a) Como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.

b) Como instrumentos. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas (Guibourg et al., 2006). Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear

documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

2.2.10.3.7. Daños o modificaciones de programas o datos computarizados

a) Sabotaje Informático. El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variado y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección. Básicamente, se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

b) Conductas dirigidas a causar daños físicos. El primer grupo comprende todo tipo de conductas destinadas a la destrucción «física» del hardware y el software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc. En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

c) Conductas dirigidas a causar daños lógicos. El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos «lógicos», o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático.

Este tipo de daño a un sistema se puede alcanzar de diversas formas. Desde la más simple que podemos imaginar, como desenchufar el ordenador de la electricidad mientras se está trabajando con el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo. Según

Arbulú (2002): “Estos programas destructivos, utilizan distintas técnicas de sabotaje, muchas veces, en forma combinada” (p. 111). Sin pretender realizar una clasificación rigurosa de estos métodos de destrucción lógica, se pueden distinguir a los siguientes:

- **Virus**

Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

- **Gusanos**

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

- **Bombas lógicas (Time Bombs)**

En esta modalidad, la actividad destructiva del programa comienza tras un plazo, sea por el mero transcurso del tiempo (por ejemplo, a los dos meses o en una fecha o a una hora determinada), o por la aparición de determinada señal (que puede aparecer o puede no aparecer), como la presencia de un dato, de un código, o cualquier mandato que, de acuerdo a lo determinado por el programador, es identificado por el programa como la señal para empezar a actuar.

d) Estafas electrónicas. La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que

cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra. No obstante, seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los cs en los que la operación se hace engañando al ordenador. Entre los tipos más conocidos de estafa electrónica tenemos:

- **"Pesca" u "Olfateo" de claves secretas**

Los delincuentes suelen engañar a los usuarios nuevos e incautos de la Internet para que revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio. Los "sabuesos" utilizan programas para identificar claves de usuarios, que más tarde se pueden usar para esconder su verdadera identidad y cometer otras fechorías, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

- **Estratagemas**

Los estafadores utilizan diversas técnicas para ocultar computadoras que se "parecen" electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos. El famoso pirata Mitnick se valió de estratagemas en 1996 para introducirse en la computadora de la casa de Tsutomo Shimamura, experto en seguridad, y distribuir en la Internet valiosos útiles secretos de seguridad.

- **Juegos de Azar**

El juego electrónico de azar se ha incrementado a medida que el comercio brinda facilidades de crédito y transferencia de fondos en la Red. Los problemas ocurren en países donde ese juego es un delito o las autoridades nacionales exigen licencias. Además, no se puede garantizar un juego limpio, dadas las inconveniencias técnicas y jurisdiccionales que entraña su supervisión.

- **Fraude**

Ya se han hecho ofertas fraudulentas al consumidor tales como la cotización de acciones, bonos y valores o la venta de equipos de computadora en lugares donde existe el comercio electrónico.

- **Blanqueo de Dinero**

Se espera que el comercio electrónico sea el nuevo lugar de transferencia electrónica de mercancías o dinero para lavar las ganancias que deja el delito, sobre todo si se pueden ocultar transacciones.

- **Copia ilegal de software y espionaje informático**

Se engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información. Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apoderamiento es el mismo programa de computación (software) que suele tener un importante valor económico.

- **Infracción de los derechos de autor**

La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.

- **Infracción del copyright de bases de datos**

No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.

- **Uso ilegítimo de sistemas informáticos ajenos**

Esta modalidad consiste en la utilización sin autorización de los ordenadores y los programas de un sistema informático ajeno. Este tipo de conductas es comúnmente cometido

por empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias a su trabajo.

En estos supuestos, sólo se produce un perjuicio económico importante para las empresas en los casos de abuso en el ámbito del teleproceso o en los casos en que las empresas deben pagar alquiler por el tiempo de uso del sistema.

2.2.11. Delitos informáticos en el Perú.

2.2.11.1. Generalidades. Los problemas que las innovaciones tecnológicas introducen en la sociedad, conforman una temática que origina la necesidad de la existencia de elementos típicos (descriptivos y normativos) que permitan legislar adecuadamente las acciones informáticas y telemáticas que deben ser prohibidas con precisión. Para lo cual creo que es necesario fortalecer la conciencia jurídica iberoamericana, para este tipo de delitos, lo cual sería beneficioso que tengan una represión penal con elementos comunes entre los diversos países, de forma tal que pueda haber una sanción eficaz aun cuando se cometan simultáneamente por medios telemáticos en distintos Estados.

Para tratar el tema de Delito Informático es conveniente delimitarlo jurídicamente en forma inicial definiéndolo como la realización de una acción que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea de hardware o de software.

En nuestro país y en la mayoría de países iberoamericanos existen determinadas conductas novedosas que implican una nueva criminalidad o comportamiento delictivo. Con la expresión “criminalidad mediante computadoras se alude a todos los actos antijurídicos según la ley vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos”

Como en otros sectores del Derecho Informático, la regulación jurídica de la criminalidad informática presenta determinadas peculiaridades, debidas al propio carácter innovador que las tecnologías de la información y la comunicación presentan. En el plano de la Dogmática Jurídico-penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales, obligando a revisar los elementos constitutivos de gran parte de los tipos penales existentes.

2.2.11.2. Delitos informáticos en la legislación penal peruana

2.2.11.2.1. Antecedentes normativos. Siguiendo esta técnica legislativa, y en atención a los vacíos legales existentes en esta materia tan especializada, es que mediante la disposición introducida por la anterior Ley 27309 de fecha 17 de julio del 2000, se modificó el Título V, del Libro Segundo del C.P., "Delitos Informáticos", que como señala Blossiers (2000) "sólo constituye un sector parcial de este género delictivo, orientado específicamente al ámbito patrimonial" (p. 176).

Por la similitud del anterior texto punitivo peruano, sobre lo tipificado anteriormente en el Código penal, cabe considerar que tuvo como fuente directa a lo contemplado en el proyecto de "ley informática" del Ministerio de Justicia de Chile (1986), que establecía que: "cometerá delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadores o red de computadoras o cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información. También comete este tipo de delito el que a sabiendas y sin autorización intercepta, interfiere, recibe, usa, altera, daña o destruye una computadora, o un sistema de red.". El Título contuve la siguiente clasificación típica de delitos informáticos al respecto:

Acceso indebido a base de datos, sistema o red de

Computadoras .....Art. 207 – A

Sabotaje Informativo.....Art. 207 – B

Circunstancias agravantes.....Art. 207 – C

Resulta atípico que el legislador haya decidido ubicar la sistemática de los delitos informativos dentro de los delitos contra el patrimonio, sin tener en cuenta que se incluye la protección de la intimidad en una de sus modalidades. El fundamento, debió ser agrupar en un solo capitulo el empleo de los medios informativos sin importar la afectación de distintos bienes jurídicos, ya que como hemos descrito, el delito informativo es un delito pluriofensivo.

Seguidamente, pasaremos a abordar los delitos informáticos en la legislación penal. No es nuestro interés realizar una crítica sobre los problemas sistemáticos en que el legislador ha incurrido en la elaboración de dicho o en la falta de conocimientos jurídico – penales, no obstante, su correspondiente análisis constituirá el inicio para la consagración de la debida protección penal de la seguridad informática, para que de este modo se pueda realizar modificaciones a la Ley N° 27309 – "Ley de Delitos Informativos", las mismas que creemos que son necesarias.

c. Tipificación penal de delitos informáticos derogados

Acorde a lo tipificado anteriormente sobre los ilícitos informáticos que se contemplaron en torno al Código Penal Peruano acerca de los derogados Artículos 207 – A, 207 – B y 207 – C, se tuvo al respecto lo siguiente:

- **Interferencia, acceso o copia ilícita contenida en base de datos**

Artículo 207º-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

a) Bien jurídico tutelado

Es la intimidad y el patrimonio. Ahora bien, podríamos señalar que el bien jurídico protegido en ese delito es el patrimonio, la intención del legislador parecería haber sido la configuración de un delito de peligro abstracto. No denotar que el bien jurídico protegido en este delito es el patrimonio, sino más bien, preliminarmente, la intimidad.

Ello a consecuencia que en tipo no se exige que el sujeto tenga la finalidad de obtener un beneficio económico, este requisito si bien no es constitutivo de la modalidad agravada, más no de la conducta delictiva descrita en el tipo básico, ya que el legislador considera el mero ingreso no autorizado como afectación a la intimidad.

b) Tipo objetivo de lo injusto

El sujeto activo y pasivo puede ser cualquiera. La conducta prohibida consiste en el empleo (desde dentro) o penetración (desde afuera) indebida a la base de datos, sistemas informativos o red de computadoras.

c) Tipo subjetivo de lo injusto

Es doloso. Si el agente actuó con la finalidad de obtener un beneficio económico así no lo consiga el tipo se agrava.

d) **Iter criminis**

Este delito se consuma con el ingreso o utilización de base de datos, sistemas informativos o red de computadoras Delito de mera actividad.

e) Incidencia del ilícito en el Perú

La comisión frecuente del delito de la interceptación de datos informáticos en el Perú, se ha venido constituyendo cada vez en una grave amenaza contra la libertad de expresión, y

que en recurrentes casos ya se ha tendido a vulnerar el ejercicio del derecho a la intimidad o a la privacidad.

Tras los casos de chuponeo informático, o de acciones ilícitas de hackers en acceder indebidamente a datos de información privada de Altos funcionarios Públicos del Estado Peruano; teniéndose el caso de que en el año 2010 el Estado llegó a denunciar y procesar penalmente tal ilícito ante el Tribunal Judicial Competente, y de que además sea sancionada (tanto a los medios como a quienes las obtuviera). Sin embargo, dentro de este punto el Tribunal Constitucional de nuestro país indicó que se debe tener en cuenta que la información obtenida obedece a intereses públicos o privados.

Según la vigente Constitución Política del Perú, se tiene que la sola intromisión a la esfera privada de una persona debe ser sancionada. Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de data crédito), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros.

Como casuística importante del ilícito tratado, se tiene el caso del 2012 del periodista del Diario El Comercio, Rudy Palma Moreno que fue denunciado por cometer el ilícito de interceptación de datos informáticos sobre Altos Funcionarios Estatales; en que tal periodista denunciado, venía trabajando desde el año 2006 en el diario Perú 21 perteneciente al grupo El Comercio; siendo que desde la sala de redacción se las ingeniaba para acceder a los correo electrónicos de ministros y funcionarios de gobierno para obtener información de primea mano. El miércoles 25 de abril del 2012, los investigadores de la división de delitos informáticos de

la dirección de Investigación Criminal (DIRINCRI) quedaron asombrados por la cantidad de información encontrada en su cuenta de correo.

La Oficina de Informática del Mincetur detectó que el correo del entonces titular de dicho ministerio, José Luis Silva Martinot, había sido interceptado, y que desde tal dirección electrónica "se obtuvieron mensajes adulterados" desde el 16 de abril. Dichos mensajes tenían origen en una cuenta de correo electrónico que hacía reenvíos de correos electrónicos a la cuenta electrónica de la esposa de un alto funcionario, atribuyéndole "conductas morales inapropiadas y hostilizándola, haciéndole conocer que viene siendo objeto de un reglaje", dice el documento judicial. Un informe técnico de dicha oficina del Mincetur detectó que se había accedido remotamente a la cuenta del funcionario desde una sola dirección IP", y que pertenecía a la Empresa Editora El Comercio. Comprobaciones hechas con el encargado de sistemas de esta empresa, confirmaron que la computadora detectada "es la asignada al denunciado Rudy Eric Palma Moreno".

El 25 de abril del 2012, los agentes de la DIVINDAT, al mando del entonces comandante PNP Luis Lazo, llegaron a las oficinas del diario Perú.21, para revisar la computadora que usaba Palma y comprobaron que poco antes había ingresado ilegalmente a la red del Mincetur. Se procedió a la detención de Rudy Eric Palma Moreno (35), en flagrante delito, en razón de que al efectuarse la revisión de la PC asignada por su empleadora (Diario Perú.21), se encontró intrusismo indebido remoto a la red de computadoras del Mincetur con fecha 25 de abril de 2012, precisa el atestado. El atestado policial señaló que el 30 de abril, la Policía no pudo llevar a cabo el Acta de Constatación del recojo de los archivos "Log" de acceso remoto a la computadora asignada a Rudy Palma, en las instalaciones de la empresa editora El Comercio S.A.

Recién se formuló el Acta de Constatación el 30 de abril 2012, respecto al recojo de los archivos "Log" de acceso remoto a la computadora asignada al detenido: Rudy Eric Palma

Moreno, (…), diligencia que no se pudo llevar a cabo ante la negativa de Karim Merzthal Reyes, representante legal de la empresa Editora El Comercio S.A., quien señaló que daría respuesta al oficio con el cual se solicita la diligencia, negándose a firmar el acta, lo que conforme se expresaba en el documento policial correspondiente.

En el apartado de "Análisis de los hechos" la Policía sostiene que Palma no estaba solo en el espionaje informático. "Por otro lado, obra como prueba del ilícito investigado el Acta de Visualización de Cuenta de Correo Electrónico del 02MAY2012; nos permite deducir la participación de terceras personas en los ilícitos investigados y que estarían coludidos con el detenido", dice el documento. Rudy Palma, quien en todo el proceso se niega a proporcionar sus identidades; motivo por el cual se solicitó el levantamiento del secreto de sus comunicaciones, respecto a las cuentas siguientes de correos electrónicos:

- gcmincetur@gmail.com,
- gcmincetur15@gmail.com,
- silvagutierrezmincetur@gmail.com,
- minceturcarrillo@gmail.com,
- carrillogonzalo100@gmail.com y
- rpmoreno@gmail.com", indica el atestado.

Por la forma y las circunstancias de los hechos, se infiere que de todo ello tendría pleno conocimiento el director del diario 'Perú.21', Fritz Du Bois, y la editora Gina Sandoval, a quien el detenido le reportaba diariamente las fuentes de información obtenida, conforme a lo manifestado por el propio Du Bois", según información revelada del respectivo informe policial. Se precisa asimismo que la Srta. Gina Sandoval no cumplió con presentarse a la Dirincri para esclarecer los hechos. "Editora (Gina Sandoval) que, pese a haber sido notificada no ha cumplido con presentarse a esclarecer su participación en los hechos denunciados e

investigados, por lo que junto al referido director del diario 'Perú.21' resultan implicados de los hechos", según detalle informativo del propio atestado policial.

El documento remarca también que no se ha podido establecer la responsabilidad o no en los hechos de la editora de cierre de "Perú.21", Claudia Yzaguirre. "Con relación al grado de participación y responsabilidad de Claudia Yzaguirre Godoy, Editora de Cierre del diario Perú.21, (…), no se ha podido establecer su responsabilidad o no en los hechos en razón de que por la premura de la investigación no se ha podido citarla (…), por lo que la autoridad competente deberá pronunciarse de acuerdo a (…) ley", según el informe policial.

El Poder Judicial actuó con la celeridad procesal requerida, dado que el Juzgado Penal de Turno Permanente de Lima abrió la instrucción pertinente con orden de detención contra el periodista Rudy Erick Palma Moreno, como presunto autor del delito contra el patrimonio, delito informático en la modalidad de utilización indebida del sistema informático en agravio de varios ministerios. De igual manera ordenó la detención de Gina Elizabeth Sandoval Cervantes, editora de economía del diario Perú 21, como presunta cómplice primario de Palma Moreno por el delito contra el Estado y la Defensa Nacional, y rebelión de secretos de Estado. Palma Moreno, que también es acusado del delito contra la libertad y violación de correspondencia en agravio de altos funcionarios del gobierno como el ministro de Comercio Exterior y Turismo, José Luis Silva Martinot; ya había sido despedido dicho periodista del referido diario; aunque la prensa periodística Perú 21 llegó a calificar de arbitraria la orden de detención contra Elizabeth Sandoval, alegando que Rudy Palma violó deberes de su función al utilizar su computadora de trabajo para ingresar a cuentas personales de diversas autoridades.

Según el documento de la denuncia, y por acceso a fuentes judiciales, Palma fue denunciado por delito contra el patrimonio, por la comisión de "delito informático en la modalidad de utilización indebida del sistema informático". A Palma se le imputó de "haber ingresado y utilizado de manera indebida información contenida en el sistema o red de

computadoras" de entidades estatales como el Ministerio de Comercio Exterior y Turismo (Mincetur), Ministerio de Economía y Finanzas (MEF), Ministerio de la Producción (Produce), Presidencia del Consejo de ministros, Ministerio de energía y Minas y PromPerú, dice el texto. Se indicó que tales acciones ilícitas buscaban "utilizar la información obtenida en beneficio personal", para lo que ingresó a los servidores de correo "con la finalidad de interceptar los mensajes y descargar los archivos adjuntos de las cuentas de correo de diversos funcionarios" de las mencionadas entidades del Estado.

Palma también fue denunciado por el delito contra La Libertad, en su modalidad de violación de la correspondencia, por "abrir indebidamente" las cuentas de correo del ministro de Comercio Exterior y Turismo, José Luis Silva Martinot, otros funcionarios de este despacho y demás ministerios. La denuncia explica que Palma se apropió de las contraseñas de acceso a los correos de dichos funcionarios para descargar documentos "que se encontraban adjuntos a las cuentas de correo de la red de computadoras de entidades públicas". Otro delito por el que ha sido denunciado Palma es contra el Estado y la Defensa Nacional, en la modalidad de revelación de secretos nacionales. La denuncia acredita que el periodista reveló secretos de Estado "que exigen ser guardados por ser de interés de la Nación". Los temas revelados por Palma están referidos a un convenio algodonero, publicado en una nota periodística, y a una resolución legislativa que autorizaba el ingreso de tropas extranjeras al país, asuntos que constituyen "información de carácter secreto, cuya revelación afectaría los intereses del Estado".

El periodista denunciado como procesado, estuvo detenido por 8 días. El primer día mientras era interrogado, el diario Perú.21 se deshizo rápidamente del redactor Rudy Palma, al despedirlo luego que fue descubierto y detenido por haber espiado correos electrónicos de altas instancias gubernamentales, pero sostiene que el posible acto ilegal se limita a la actividad personal del reportero y rechaza más implicancias. Por ello, un pronunciamiento del periódico

llegó a rechazar la orden de detención de la editora de la sección Economía de dicho periódico, Gina Sandoval, por considerar que el proceso iniciado contra la periodista “es absolutamente ilegal”, y calificó como “arbitrariedad” la decisión judicial.

En una nota publicada ante la citada orden, el periódico afirmó que en ningún momento objetó la investigación iniciada al periodista Rudy Palma, detenido en la sede de la Dirección de Investigación y Criminalística (Dirincri) y despedido por el diario. El Diario Perú 21 alegó también que considerar a Sandoval como cómplice en los hechos “por el simple hecho de ser editora del medio, es totalmente irregular”, y que no se presentará ante la justicia mientras no tenga garantías. En el tema hay una contradicción, pues mientras la Policía, la fiscalía y la jueza a cargo plantearon que Sandoval no acudió cuando fue llamada a declarar y dicen tener constancia de ello, el pronunciamiento sostiene que no fue formalmente citada. Resalta que tanto la empresa que produce el periódico, Prensa Popular, como su director, Fritz Du Bois, han colaborado “activamente” con las autoridades judiciales y la Policía, que lo sometió a un largo interrogatorio.

Se agrega además que cuando Du Bois fue a declarar a la Dirincri, “en ningún momento fue informado de que hubiese alguna notificación o requerimiento de información hacia otro miembro del equipo del diario que dirige”. La empresa más bien sostuvo estar “alerta sobre el caso en cuestión y que continuará, como lo ha hecho hasta ahora, colaborando con las autoridades judiciales para esclarecer los hechos”. Según el atestado policial Nº 071 de la Dirección de Investigación Criminal (Dirincri) de la Policía Nacional del Perú, el periodista Rudy Palma ingresó indebidamente y en varias oportunidades a la red de computadoras de los ministerios de Comercio Exterior y Turismo (Mincetur), de Economía y Finanzas (MEF), de Energía y Minas (Minem), y de Producción (Produce), para extraer y copiar documentos de altos funcionarios estatales.

El informe Policial refiere, además, que entre otras instituciones estatales afectadas también figuran la Presidencia del Consejo de ministros (PCM), y la Comisión de Promoción del Perú para la Exportación y el Turismo (Promperú). Por ello, la jueza Delia Flores aperturó instrucción al imputado Rudy Palma por los delitos contra la libertad-violación de la correspondencia en agravio de funcionarios gubernamentales, contra el Estado y la Defensa Nacional-Revelación de Secretos Nacionales en agravio del Estado El atestado policial también precisó que se había utilizado el equipo analizado, en cuanto al caso de la computadora del diario "Perú.21" que se asignó a Rudy Palma, para acceder indebidamente a las siguientes fuentes electrónicas:

- A la red de computadoras de mincetur.gob.pe,
- produce.gob.pe,
- pcm.gob.pe,
- mef.gob.pe,
- promperu.gob.pe
- minem.gob.pe, y
- presidencia.gob.pe".

Desde el equipo de cómputo asignado al detenido Rudy Eric Palma Moreno por su empleadora empresa 'PRENSA POPULAR SAC', editora del Diario Perú.21", para el mejor desempeño de sus funciones periodísticas como redactor, se han efectuado diversos accesos remotos no autorizados a correos electrónicos del Mincetur y el MEF", conforme indicaba el documento de informe policial. A continuación, se enumeran los ingresos electrónicos realizados en forma cronológica, desde:

- El 8 de abril de 2012 hasta el 25 de abril de 2012.
- El 8 de abril de 2012 a horas 11:43 a.m., (Rudy Palma y otros cómplices por determinar) accedan al servidor de correo MINEM.GOB.PE, precisa.

- El 15de abril de 2012 a horas 12:06 pm, se encontró un rastro de acceso a correo de dominio MINCETUR, cuyo contenido es: Re: MINISTRO el lunes nos entrevista en vivo Fox Sports por Dakar.
- El documento refiere que el 16 de abril de 2012 a horas 04:19 pm, accesan al servidor del correo MINCETUR".
- El 22 de abril de 2012 a horas 11:48 am, accesan al correo web.produce.gob.pe y a horas 01:17 pm, accesan al servidor de correo promperu.gob.pe.
- El 23 de abril de 2012 a horas 06:34 pm accesan al servidor de correos del MINCETUR", revela el atestado.
- El 24 de abril de 2012 a horas 10:36 am, horas: 09:10 p.m., horas: 06:34 pm, todos ellos accesados al servidor de correos MINCETUR y el mismo día a horas: 09:10 pm, se detectó un acceso directo a la cuenta de correo Juan José Gastañet" del servidor de MINCETUR", enumera el documento policial.

El día de su detención, Rudy Palma y otros presuntos implicados "a horas 02:16 pm acceden al servidor de correos electrónicos MEF.GOB.PE, a horas 07:29 pm accediendo a la cuenta de correo de SICCHA MARTÍNEZ.ROG en el servidor de correos MEF.GOB.PE, que corresponden todos ellos al servidor del Ministerio de Economía y Finanzas (MEF), se remarcó conforme al atestado policial. Se ha llegado a establecer asimismo que a través de la Dirección IP pública: 190.8.135.30, cuyo titular es la empresa Editora El Comercio S.A., se registró accesos a las diferentes cuentas de correos electrónicos corporativos de altos funcionarios de MINCETUR y del MEF", conforme se sostenía en base al documento del informe policial correspondiente; se adiciona también que las investigaciones arrojaron que los accesos remotos fueron realizados por el usuario Rudy Palma.

"Se conoció que dichos accesos remotos fueron realizados por el usuario: PALMORER desde la computadora asignada con la dirección IP (LAN) 172.30.61.125 correspondiente al

detenido Rudy Eric Palma Moreno desde el 01 de abril 2012 al 24 de abril de 2012, según se precisaba en el atestado elaborado por la División de Investigación de Delitos de Alta Tecnología (Divindat). Los investigadores corroboraron que el "hackeo" se realizó desde la computadora de Rudy Palma al recibir los reportes impresos de la empresa Editora El Comercio S.A. "Los reportes impresos que esta misma empresa llegó a ofrecer a Mincetur y que fuera presentada como prueba a su denuncia, de lo que se desprende que fue éste el mismo que remitió mensajes electrónicos a diversos funcionarios a través de la creación de las cuentas de correo electrónico: gcmincetur@gmail.com y gcmincetur15@gmail.com bajo la falsa identidad de Gonzalo Carrillo, con el fin de no identificarse, ante los titulares de las cuentas de correos corporativos de Mincetur".

La policía detectó que Rudy Palma extrajo y copió 587 archivos digitales de los correos corporativos de funcionarios del Mincetur, del MEF, de Produce y de otros organismos estatales. "En la carpeta Descargas del usuario PALMORER (Rudy Palma), que es el repositorio por defecto de los archivos descargados en línea, se han encontrado un total de Quinientos Ochenta y Siete (587) archivos digitales que han sido descargados, señala el atestado. El documento agrega que el procurador adjunto del Ministerio de Economía, Ángel Vivanco Ortiz (57), y el director general de la Oficina de Administración de Economía, Roger Siccha Martínez (60), se presentaron en la Dirincri como parte agraviada para denunciar que esa cartera fue también hackeada por Rudy Palma.

Además, se tiene que otros funcionarios del Ministerio de Economía y Finanzas, como Ángel Augusto Vivanco Ortiz y Roger Alberto Siccha Martínez, al conocer los hechos y al haber evidencias de accesos indebidos a su servidor web de correos electrónicos (de Economía), por el detenido Rudy Eric Palma Moreno, se constituyeron a esta unidad policial, se apersonaron como parte agraviada denunciando el hecho", ello conforme se indica en el atestado policial. Mientras entretanto, la entonces Oficina de Control de la Magistratura

(OCMA) dispuso también abrir una investigación preliminar a la jueza Delia Flores, “por haber ordenado arbitrariamente la detención de la editora de la sección economía del diario Perú.21”, Gina Sandoval, a quien se le atribuye ser cómplice de Rudy Palma en la revelación de secretos de Estado”, según comunicado de dicho organismo funcionable por aquellos momentos. “Es inaceptable que se haya ordenado su detención sin concederle jamás la oportunidad de contestar a ningún interrogatorio, pretendiendo que se ha negado a acatar supuestas notificaciones que jamás recibió”, sostuvo el informe de la OCMA.

Finalmente, según las investigaciones policiales, se llegó a que no se pudo concluir efectivamente que se hayan revelado secretos de tal tipo, en que el imputado Rudy Palma era redactor en la sección economía y los temas que trataba eran referentes a materia empresarial y precios de productos, entre otras cosas. Palma fue acusado de violación de correspondencia, es cierto que el periodista violó correspondencia electrónica de un funcionario público al ingresar a su e-mail sin autorización.

Sin embargo, nuevamente aquí entra en juego los vacíos legales que se tenían por entonces dentro del código penal, en lo que correspondió se le llegó a imputar conforme a su artículo 161, dejándose entrever la confusión de que si había accedido indebidamente a material informático de correos electrónicos, o de si había accedido a documentos físicos de correspondencia, tales como hojas de papel, cartas, entre otros; por lo que a lo más pudo recibir una pena de prisión de dos años, pero ante la arraigada confusión que se generó sobre qué delito se le debió imputar específicamente al sujeto denunciado, en función del acto de ingresar indebidamente a los correos electrónicos que no llegan a ser de uno mismo; y que ante la falta de precisión del tipo penal imputable, es por ello que Rudy Palma finalmente fue absuelto y salió en libertad, decisión que fue tomada por la Jueza del 50° Juzgado Penal de Lima, Lorena Alessi.

- **Alteración, daño o destrucción de base de datos**

Artículo 207º-B.- El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

a) Bien jurídico tutelado

El patrimonio. Por la ubicación que le ha dado el legislador en nuestro Código Penal, con el delito de intrusismo informático, el Estado pretende cautelar el patrimonio. Ello debido que la información en tránsito o contenido en una base de datos, un sistema o red de computadoras, en la actualidad es susceptible de valoración económica. En consecuencia, al configurarse cualquiera de las conductas denominadas en conjunto hacking lesivo, se ocasiona daño económico o patrimonial al dueño o titular de la base de datos, sistema o red de computadoras. Así la conducta del agente no esté dirigida a obtener un beneficio económico personal, su propia realización en forma automática ocasiona un perjuicio patrimonial a la víctima o sujeto pasivo.

En ese sentido, no compartimos posición con Durand Valladares cuando sostiene que de la lectura del tipo penal se puede advertir que el bien jurídico protegido en este delito no es el patrimonio, sino más bien, preliminarmente, la intimidad. El tipo no exige que el sujeto tenga la finalidad de obtener un beneficio económico, este requisito es constitutivo de la modalidad agravada, más no de las conductas descritas en el tipo básico, ya que el legislador considera el mero ingreso no autorizado como afectación a la intimidad. No obstante, concluye el citado autor, el bien jurídico protegido en estos delitos es la seguridad informática y no el patrimonio ni la intimidad.

b) Tipo objetivo de lo injusto

El sujeto activo y pasivo puede ser cualquiera.

La conducta prohibida consiste en utilizar, ingresar o interferir indebidamente a una base de daros, sistemas informativos, red o programas de computadoras con el objeto de alterarlos, dañarlos, o destruirlos.

c) Tipo subjetivo de lo injusto

Es dolo.

El delito de intrusismo informático o acceso informático indebido se configura cuando el agente o autor utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito contenida en una base de datos.

El tipo penal 207-A recoge varias conductas delictivas que por sí solas o agrupadas configuran el delito de intrusismo informático, acceso informático indebido o hacking lesivo. En tal sentido, las conductas típicas y antijurídicas podemos identificarlas en las siguientes:

1. Utilizar; usar; aprovechar o emplear indebidamente una base de datos, sistema o red de computadoras para diseñar un esquema u otro similar.
2. Utilizar, aprovechar, emplear o usar indebidamente una base de datos, sistema o red de computadoras para ejecutar un esquema u otro similar.
3. Utilizar, usar; emplear o aprovechar indebidamente una base de datos, sistema o red de computadoras para alterar un esquema u otro similar.
4. Utilizar, usar, emplear o aprovechar indebidamente una base de datos, sistema o red de computadoras para interferir información en tránsito o contenida en una base de datos.
5. Utilizar, emplear, aprovechar o usar indebidamente una base de datos, sistema o red de computadoras para interceptar información en tránsito o contenida en una base de datos.
6. Utilizar, emplear, aprovechar o usar indebidamente una base de datos, sistema o red de computadoras para acceder a información en tránsito o contenida en una base de datos.

7. Utilizar, usar, aprovechar o emplear indebidamente una base de datos sistema o red de computadoras para copiar información en tránsito o contenida en una base de datos.
8. Ingresar, introducir, entrar o infiltrarse indebidamente una base de datos, sistema o red de computadoras para diseñar un esquema u otro similar.
9. Ingresar, entrar, infiltrar o introducirse indebidamente una base de datos, sistema o red de computadoras para ejecutar un esquema u otro similar.
10. Ingresar, entrar, introducir o infiltrarse indebidamente una base de datos, sistema o red de computadoras para alterar un esquema u otro similar.
11. Ingresar, introducir, infiltrar o entrar indebidamente una base de datos, sistema o red de computadoras para interferir información en tránsito o contenida en una base de datos.
12. Ingresar, infiltrar, introducir o entrar indebidamente una base de datos, sistema o red de computadoras para interceptar información en tránsito o contenida en una base de datos.
13. Ingresar, infiltrar, introducir o entrar indebidamente una base de datos, sistema o red de computadoras para acceder a información en tránsito o contenida en una base de datos.
14. Ingresar, entrar, infiltrar o introducirse indebidamente una base de datos, sistema o red de computadoras para copiar información en tránsito o contenida en una base de datos.

De esa forma, las siete últimas conductas prohibidas se configuran cuando el agente, se introduce, entra o ingresa indebidamente a una base de datos, sistema o red de computadoras. Aquí el agente no está haciendo uso del sistema o red de ordenadores, de un momento a otro ingresa sin autorización. El ingreso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones. El agente puede aprovechar la falta de rigor de las medidas de seguridad para introducirse o ingresar o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos, se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en

los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

En concreto, estos supuestos se configuran cuando el usuario, sin autorización ni consentimiento del titular del sistema, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico) o hace la conexión por accidente, pero voluntariamente decide quedarse o mantenerse conectado. Se produce la interceptación no autorizada, por ejemplo, cuando el haber o pirata informático detecta pulsos electrónicos trasmitidos por una rede o una computadora y obtiene información no dirigida a él. En tanto que las demás conductas se configuran cuando el agente ya estando dentro o haciendo uso del sistema o red de computadoras, indebidamente o sin autorización comienza a usar, utilizar o aprovecharse en beneficio personal de la información o datos que brinda el sistema o red de computadoras.

Por ejemplo, se configura el delito cuando el agente reproduce o copia programas informáticos sin contar con la autorización o consentimiento de titular del programa. Otro dato objetivo que debe concurrir en las conductas para configurarse los supuestos delictivos en hermenéutica jurídica es que el agente o autor de los comportamientos ilícitos, debe actuar en forma indebida, o sin autorización. Es decir, el agente al desarrollar la conducta típica debe hacerlo sin contar con el consentimiento del titular o responsable de la base de datos, sistema o red de computadoras. Si llega a verificarse que el agente actuó contando con el consentimiento del titular de la base de datos, por ejemplo, la tipicidad de la conducta no aparece.

De esa forma, debe quedar claramente establecido que “el carácter indebido que califica, precisamente, la conducta constituye un elemento del tipo, por lo que su ausencia no ha de ser apreciada como causa de justificación sino de atipicidad. Finalmente, en cuanto a la tipicidad objetiva, resulta irrelevante determinar el móvil o propósito del agente o autor de los

comportamientos delictivos descritos. Solo si se verifica que el autor actúa movido o guiado con el propósito de conseguir un beneficio económico, la conducta se agrava como veremos más adelante al analizar el segundo párrafo del artículo 207-A del Código Penal.

d) Circunstancias cualificantes agravantes

Artículo 207º-C.- En los casos de los Artículos 207º-A y 207º-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

- El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
- El agente pone en peligro la seguridad nacional.

Si el agente realiza o desarrolla cualquiera de las conductas ya analizadas con el fin o propósito de obtener un beneficio económico, se configura la agravante del delito de intrusismo informático previsto en el segundo párrafo del artículo 207-A del Código Penal. Aquí el autor o agente de los delitos informáticos merece mayor sanción por haber actuado guiado o movido por la finalidad concreta de obtener un beneficio económico personal en perjuicio evidente de la víctima.

2.2.12. Aspectos sustantivos sobre los delitos informáticos

2.2.12.1. Ley N° 30096. ley de delitos informáticos.

2.2.12.1.1. Capítulo I: Finalidad y Objeto de la Ley

a) Artículo 1°: Objeto de la Ley

Nos ampararnos en la amplitud conceptual de Téllez, evitando pugnas doctrinarias estériles, propias de la intolerancia. Así pues, en general, los delitos informáticos son “actitudes ilícitas que tienen a las computadoras como instrumento o fin”. En el pensamiento de Eduardo Rosende, habrá conflicto informático cuando mediante cualquier actividad que involucre el procesamiento automático de datos, se afecten de forma grave derechos de terceras personas. Vistas, así las cosas, no resulta extraño que una ley de delitos informáticos tipifique conductas

específicas, particularmente graves, que están dirigidas contra el bien jurídico "información" o contra otros bienes jurídicos, si es que para su afectación ha estado involucrado el procesamiento automático de datos. Más que una ley sustentada en la necesidad de ejercer la función punitiva del Estado enfocada en la protección de un bien jurídico específico, ya sea éste novedoso o no, esta ley tiene como principal objetivo la estandarización de la ley penal peruana con el orden penal internacional determinado, principalmente, por la Convención contra la Cibercriminalidad del Consejo Europeo (CETS 185), conocida también como Convención de Budapest. De hecho, la octava disposición complementaria final evidencia esta intención normativa. El camino planteado es el correcto, si es que en realidad se pretende una adhesión en los términos que la propia Convención determina, ya que ésta tendrá que pasar satisfactoriamente por exigentes filtros financiados y establecidos por el propio Consejo Europeo. No hay que dejar de tener en perspectiva que el texto de la Convención de Budapest plantea estándares normativos, por lo que corresponde que los países adherentes verifiquen, mediante una revisión introspectiva, si sus respectivas legislaciones penales nacionales cumplen con este estándar o si se necesitan retoques para afinar la estandarización.

Al respecto, cabe señalar que la Convención, al representar un estándar mínimo que posibilita su universalización, se inclina exclusivamente por la sanción de las conductas dolosas, vale decir de aquellas cometidas con conocimiento y voluntad de realizar el acto punible y de obtener el resultado dañoso. En el caso peruano, los tipos penales no tienen que especificar reiterativamente en todos los casos que las conductas punibles tipificadas están revestidas del dolo como elemento subjetivo del tipo, ya que el artículo 12 del Código Penal determina con meridiana claridad que el agente de infracción culposa solamente es punible en los casos expresamente establecidos en la ley. Por ello, la técnica legislativa penal recomienda no abundar en aclaraciones que solo generarían redundancia innecesaria, ya que no se compromete en absoluto el estricto apego a la estandarización internacional.

2.2.13. Acerca de los aspectos sustantivos - procesales en la investigación, y procesamiento/juzgamiento sobre delitos informáticos:

El Crimen Cibernético actualmente ha tenido una proliferación masiva en la comisión de ilícitos graves que no solo atentan contra el patrimonio y la información confidencial de las personas, cuyo patrimonio privado y económico se encuentre almacenado en las redes informáticas, sino que hasta puede llegar a transgredirse bienes jurídicos más colectivos o de carácter de seguridad nacional, cuando el espionaje informático y las acciones de terrorismo cibernético acceden a información secreta y confidencial de los sistemas de Defensa y Seguridad de un Estado, obteniendo dicha información para su posterior tráfico y venta a potencias enemigas o a organizaciones criminales para perpetrar acciones indebidas, lo que puede llegar a afectar la seguridad de un país en sus diferentes campos de acción sea militar, policial, de orden público, económico o social.

Considero que los delitos informáticos, representan una amenaza muy grave para el desarrollo de la sociedad y la estabilidad de nuestras instituciones hacia el futuro, de allí, la enorme responsabilidad de formarnos y capacitarnos en el conocimiento del Hardware y Software, así como las comunicaciones que se desarrollan a través de Internet y que son utilizados dolosamente por los criminales informáticos, no existiendo por ahora, mecanismos eficaces para poder contrarrestar esta modalidad delincuencial.

Los problemas jurídicos relacionados con la Internet, se basan especialmente en los nombres de dominio y las marcas comerciales, al existir diferencias en su posesión y administración por parte de sus propietarios; de los derechos de autor, ante la imposibilidad de prohibir las reproducciones no autorizadas de trabajos y elementos de propiedad intelectual, la realización virtual de actividades altamente reguladas en los ámbitos financieros, de compra y venta de valores; al no existir fronteras ni el control adecuado sobre las incipientes instituciones mercantiles, que hacen uso de la red como sustento. El comercio electrónico desarrollo gracias

a la proliferación de la Internet, los problemas más urgentes se basan en la formación del consentimiento, la seguridad acerca de las identidades de los contratantes y la prueba de las obligaciones; como también es sobre la legislación aplicable al acto o contrato específico, los tribunales competentes y la seguridad en los medios de pago; para ello las distintas legislaciones a nivel mundial y gracias a la promulgación de la Ley Modelo sobre el Comercio electrónico, de la Comisión de las Naciones Unidas para el Derecho Comercial (UNCITRAL), que recomienda a los países integrantes de las Naciones Unidas, sobre la legislación nacional en materia de las firmas y documentos electrónicos, con el objeto de dar seguridad a las relaciones jurídicas electrónicas. Chile, en parte adopta dicho criterio, mediante el establecimiento del Decreto Supremo N°. 81, de 1999, del Ministerio Secretaría General de la Presidencia, que regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado, otorgando a la firma digital los mismos efectos que la firma manuscrita, eliminando de esta forma la necesidad de sellos, timbres y vistos buenos.

Fernández et al. (2010) concluyen que todos los avances de carácter tecnológico/informático, siempre han llegado a ser los elementos provocadores de que cambien significativamente los estilos de vida esenciales de comunicación y desarrollo de las principales actividades laborales de la sociedad humana; las que han llegado a cambiar casi de manera completa en los últimos veinte años, habiendo surgido cada vez más la tipificación punitiva de nuevas figuras penales, debiéndose a que anteriormente no existían los grandes avances tecnológicos - informáticos como electrónicos y comunicacionales en base a las altas exigencias como ventajas tecnológicas que se tienen actualmente; habiéndose desarrollado las conclusiones pertinentes, tales como en primer lugar, de que se haya estado dando de manera paralela el desarrollo de grandes avances informáticos - tecnológicos, a la vez también se ha estado perfeccionando indebidamente el desarrollo de nuevos modus operandi sofisticados y especializados de los propios sujetos criminales, dado que estos, viven a la vanguardia moderna

de poseer cada vez más conocimientos tecnológicos de avanzada, que tienden aprovechar ilegalmente para cometer nuevos actos delictivos cada vez más eficaces, difíciles de rastrear y que les reporten ingentes beneficios económicos; y como segunda conclusión, se tiene que a causa originalmente de la carencia de una tipificación penal más exhaustivamente completa de los delitos perpetrados con uso indebido de los medios tecnológicos/informáticos, y que por un buen periodo de tiempo, los cibercriminales venían cometiendo una diversidad de acciones delictivas – informáticas, quedando impunes al no recibir penas condenatorias al respecto, y que la única manera de evitarse ser víctimas de tales ilícitos en aquellos momentos, era de aconsejarse a los ciudadanos que realizaban transacciones económicas y comerciales por vía informática, en adoptar todas las medidas de seguridad electrónica que sean necesarias al respecto.

Los delitos informáticos, antes de la vigencia aplicativa de la Ley N° 30096 del 2013, se constituían en un gran vacío jurídico para la legislación penal peruana, y que ante la diversidad comisiva de delitos por medio virtual, se tenía una gran lista enumerable de todos los delitos informáticos que no se encontraban tipificados por entonces en nuestro Código Penal y que era materia de arduo debate por parte de especialistas en materia informática, así como por académicos, penalistas y legisladores; y que llegaría a tratarse en nuestro país, a comienzos del Siglo XXI, por parte del Congreso de la República, que llegaría a promulgar por primera vez dentro del ordenamiento jurídico peruano, a la primera norma penal contra los delitos informáticos, que llegó a ser la Ley N° 27309, dada el 26 de junio del 2000, que incorporó como primeras figuras delictivas informáticas dentro del Código Penal vigente, en cuanto por entonces a lo que se había tipificado en base a los artículos 207-A., referente al ilícito de la Interferencia, acceso o comisión de acto de copia ilegal respecto a todo contenido informativo almacenado en las bases de datos; mientras que como segunda figura ilícita se tipificó en torno al Art. 207-B referente al ilícito de Sabotaje Informático y en lo que concierne a lo tipificados

en torno al entonces Artículo 207-C, que penalizó las modalidades agravantes en que se podían perpetrar los ilícitos informáticos descritos en los artículos señalados anteriormente; y que de por sí resultó en una tipificación punitiva muy insuficiente, que contemplaban dentro de los enunciados jurídicos - penales de las figuras delictivas referidas, una descripción penal en términos muy técnicos que eran muy poco entendidos por los propios operadores jurídicos - penales; y que ante tal dificultad, se entendía que la ley penal debía predominar y castigar penalmente a todo mal uso de la tecnología informática moderna; bajo consideración de la premisa técnica, de que a pesar de tenerse la necesidad de contarse con los medios o herramientas de control informático que pueda atender todas las necesidades jurídicas - penales referentes en protección y penalización contra todas las modalidades de delitos informáticos en sí, pero tales herramientas jurídicas – penales que se han dado por la legislación penal y por la política criminal peruana contra los ilícitos informáticos, no resultan infalibles de por sí, porque constantemente surgen nuevos delitos de carácter informático por parte de las nuevas tecnologías informáticas y comunicacionales que van apareciendo, y a pesar de que la seguridad informática también ha evolucionado hasta la actualidad, y pese a seguir la rutina convencional de emplearse diversas capas informáticas de seguridad, considerándose la aplicabilidad de los firewall, que a pesar de tener fuertes mecanismos de seguridad tecnológica privada para asegurar la defensa proteccionista del acceso a toda la información contenida en las plataformas informáticas de las bases de datos, pero muy a pesar de ello, los firewalls no pueden llegar a proteger a las diferentes clases de brechas informáticas de seguridad que se puedan presentar indistintamente, como las brechas de tipo interna, así como las de tipo física, y de todas las intrusiones que se lleguen a ocasionar por cuestionables actos divulgables de las contraseñas relacionadas al acceso a la información privada de datos personales de las personas usuarias y/o clientes reservados, llegándose a constituir los programas firewall y los software antivirus, entre las principales medidas de seguridad informática, para evitarse constituir en

una víctima potencial de cualquier tipo de ilícito informático, aunque tales herramientas de seguridad informática no sean totalmente infalibles en sí.

En lo que corresponde a la función desempeñada por la Policía Nacional del Perú, mediante la Unidad Operativa Especializada que vendría a ser la División de Informática y Alta Tecnología de la Policía Nacional (DIVINDAT), que tiene responsabilidad en dar la resolución y efectivo esclarecimiento de todos los casos delictivos de ilícitos informáticos que se lleguen a perpetrar; y a la vez de poder llegar a efectuar con la requerida implementación de todos los cambios exigibles que sean vitales para la eficaz actividad verificable en el uso pertinente de todas las herramientas de control que sean necesarias, así como en ejecutarse todos los procedimientos que correspondan para de evaluación de riesgos, así como de ejecutarse todas las medidas protectoras que pudiesen coadyuvar hacia la debida minimización de todas las amenazas que se lleguen a presentar con la comisión de los ilícitos informáticos.

Recientemente, como consecuencia del crecimiento de las tecnologías de la información y comunicación en base a las redes sociales, se viene constatando el surgimiento de nuevas modalidades delictivas – informáticas; frente a lo cual la vigente ley penal informática peruana viene readecuándose para sancionar penalmente a todas las acciones delictivas innovadoras que puedan involucrar a los sistemas informáticos y tecnologías comunicacionales modernas, para cometerse delictivamente nuevas modalidades de ilícitos informáticos que atenten contra la privacidad de la información secreta, así como contra el patrimonio económico de los ciudadanos, y otros bienes jurídicos esenciales que resulten dañados (Villavicencio, 2015).

2.2.13.1. Intimidad. De las diversas definiciones se incluye la de Casabona que entiende por intimidad "aquellas manifestaciones de la personalidad individual o familiar, cuyo conocimiento o desarrollo quedan reservadas a su titular o sobre las que ejerce alguna forma

de control cuando se ven implicados terceros, entendiendo por tales, tanto los particulares como los poderes públicos (Casabona, 2006).

2.2.13.2. Derecho a la Intimidad. Ribagorna (1996) sostiene que el derecho a la intimidad no aparece enunciado de forma expresa y como categoría independiente en los textos constitucionales hasta fechas muy recientes. El primer texto constitucional en Europa que recogió de forma expresa el derecho a la intimidad fue la Constitución portuguesa de 1986 (art. 33.1) y posteriormente lo hizo la Constitución española de 1978 (art. 18). Anteriormente, tan sólo existieron formulaciones filosóficas y doctrinales. La elaboración doctrinal que sirve de precedente a la constitucionalización del derecho a la intimidad, concebido como "therightto be letalone" por el Juez Cooley, es decir, el derecho a ser dejado en paz, o a ser dejado solo, se originó en 1.890 cuando Warren y Brandeis publicaron un artículo sobre "TheRighttoPrivacy". Entre las formulaciones filosóficas podemos destacar la de Jeremy Bentham.

2.2.13.3. Defensa de la Intimidad. Se ha tratado de defender la intimidad como un valor en sí, es decir, con independencia de la finalidad perseguida por las conductas criminales (Ribagorna, 1996).

2.2.14. Escuelas Técnico Jurídicas Vinculantes a la Investigación

2.2.14.1. Escuela Técnico Jurídica. La dirección técnico penal de carácter jurídico queda expresada en América con la tendencia jurídico penal que tiene su asentamiento en Italia, y que los alemanes también han prestado gran atención a la tendencia dogmática - jurídica. En Italia, Carnelutti aparece como un eminente técnico-jurista, que escribió con agudeza temas alusivos a los filósofos. El señalaba con énfasis que el jurista debe pretender resolver sus asuntos del Derecho con su propia técnica, obviando todo lo extraño que tiende a la alienación sociocultural de cada una de las personas (Alcalá, 1985).

Por otra parte, señalamos la urgente necesidad de separar hoy la tendencia meramente técnica, respecto a la ciencia del deber ser del Derecho, que obviamente se llama dogmática y

por tanto no está debidamente desvinculada de la Filosofía, que es un aporte especializado para lograr entender con sapiencia las ciencias penales. Mejor aun cuando hoy en día es relevante e importante destacar la vinculación de la tecnología y la filosofía al enriquecimiento de la doctrina penal, que además contribuye a la humanización y sensibilización de los artículos de nuestro ordenamiento jurídico penal (Amoroso, 1991).

2.2.14.2. Escuela de la Antropología Criminal. Escuela Antropológica social y/o Lyon. El fundador recae en el medico y psicólogo francés Alexander Lacassgne fue uno de los opositores de la teoría Lombrosiana. Señala, que la sociedad es el factor preponderante o la causa de la criminalidad, considera, que a mayor desorganización y esta situación tiene estrecha relación con el problema, los objetivos y las hipótesis en cuanto a la personalidad formada, mayor criminalidad. Esto hace, que los estados desorganizados sean más altos la criminalidad (Toniatti, 1991).

Según Garbarino et al. (1990), en cambio los estudios sociológicos y jurídicos nos conducen a pensar que en las sociedades mejor organizadas, existe menos criminalidad. Esto implica que las sociedades tienen los criminales que se merecen, de esta manera se reafirma el carácter eminentemente social. Mayor cuando la sociedad es tolerante, frente a las insinuaciones exógenas que realizan. La sociedad desorganizada, es debida entre otros factores, a la carencia de la planificación social y económica. Recordemos que la familia puede hacer mucho entre la primera y segunda infancia y en la niñez en cambio es difícil pero no imposible. Que una deficiente conducta se logra corregir en la adolescencia, se da señala Lacassgne pero con bastante o suma dificultad.

El médico biólogo Paster señalaba, que un microbio solo prolifera en un medio adecuado, haciendo énfasis al trabajo de Lacasgne, donde el delincuente venía siendo un microbio, y actúa solamente teniendo a su disposición el medio social, ese medio ambiente propio para cometer el ilícito. Si el sujeto activo, hubiese sido preparado adecuadamente en el

seno de su hogar paterno-materno y con determinado estimulo emocional y afectivo, probablemente no entraría tan fácil en la senda del mal. Y la sociedad se ahorraría el tiempo necesario para no procesar a estas gentes, que en la práctica tenga conductas ilícitas, como consecuencia a la formación de su personalidad (Garbarino et al., 1990).

2.2.14.3. Teoría de la sociedad de riesgos. De acuerdo a Velasco (2010) en la dogmática penal actual hay un nuevo paradigma el de la "sociedad de riesgos" Se dice que la sociedad actual es una sociedad de riesgos, en la que se admiten evidentemente dentro de ciertos límites los riesgos que se derivan del tráfico rodado, ferroviario y aéreo, de la utilización de gases de la existencia de centrales nucleares, necesarias para facilitar energía eléctrica, pero que amenazan parte de la civilización, la producción y comercialización de productos de carácter alimenticio en grandes cantidades, con grave riesgo para los consumidores, la manipulación genética con peligro de selección de razas, a través de la creación de seres humanos por clonación, etc..

Baratta (1985) afirma que esta innegable realidad exige la comprensión de la sociedad. Son riesgos exigidos por la modernización e industrialización de la sociedad, que sin duda plantean y seguirán planteando nuevas necesidades al derecho penal a lo largo de los próximos años. Pues bien, como un claro fenómeno asociado a estos "nuevos riesgos" de la sociedad se encuentra la informática. No cabe duda que la informática proporcione muchos beneficios, pero al mismo tiempo origina no pocos riesgos, porque al generar una abundante información, en poco tiempo y en un espacio muy reducido, puede afectar a la esfera privada del individuo.

En este sentido la existencia de bancos de datos personales y su posible manipulación puede afectar a la intimidad de las personas. En España, afortunadamente la Ley orgánica de regulación del tratamiento automático de datos de Carácter personal, de 29 de octubre de 1992, proporciona la protección administrativa de esta información, cuidando el uso de dichos datos personales (Mir, 1992).

2.2.14.4. Teorías en relación al derecho a la intimidad. Son múltiples las teorías y posiciones doctrinales que se han esgrimido para delimitar el contenido del derecho a la intimidad. Pérez (1984), parte del planteamiento de delimitar conceptualmente la intimidad, con la que llama "noción actual de la privacy", porque considera que la intimidad y la vida privada, contienen una carga emotiva que las hace equívocas, ambiguas y dificulta la precisión de su significado, e incluso se llega a sostener que tiene una "definición introuvable" (Vitalis, 1981).

Entre las varias doctrinas referentes al tema, entre otras, se citan:

1. La Alemana de Hubmann, que reconoce tres esferas: la intim sphäre (secreto), la Privatsphäre (lo íntimo) e Individual sphäre (individualidad de la persona. Vg. nombre).
2. La Italiana de Frosini, que distingue cuatro fases de aislamiento: soledad, intimidad, anonimato y la reserva.
3. La Norteamericana de Jhon H. Shattuck, sostiene que la privacy abarca cuatro aspectos, a saber:

a) Freedom From unreasable search, libertad o seguridad frente a cualquier tipo de intromisión indebida en la esfera privada.
b) Privacy of association and belief, garantía del respeto a las opciones personales en materia de asociación o creencias.
c) Privacy and autonomy, tutela de la libertad de elección sin interferencias.
d) Information control, posibilidad de los individuos y grupos de acceder y controlar las informaciones que les atañen. La posición de Shattuck, estuvo precedida por Alain Westin.

Al menos en lo referente al control de la información que tiene toda persona sobre sí misma. Westin, lo llamó derecho al control de la información referente a uno mismo (TheRightto control information about one self); Lusky, posibilidad de controlar la circulación

de informaciones relevantes para cada sujeto y Fried, control sobre las informaciones que nos conciernen (Fried & Lusky, 1968).

2.2.14.5. Teoría de los delitos contra la honestidad. Honestidad (Del latín honestitas, átis) implica en la práctica, docencia y moderación en el desempeño de las funciones que realizan las personas, así como en sus palabras y en las múltiples funciones que efectúa cotidianamente, incluyendo su hogar. La persona decente es sinónimo de modesto y decoroso (Peña, 2010).

Velasco (2010) afirma que según el derecho babilónico de la época de Hamurabi, al que besaba a una mujer casada se le debía cortar el labio inferior. Según el derecho indio, se hacía culpable de adulterio el que no se conducía decentemente con una mujer ajena o le hacía indicaciones equivocas. Según Peña (2010) en la sociedad alemana de la época en que se escribió esa información, la figura jurídica honestidad estaba referida, exclusivamente, al honor, disciplina, lealtad y honestidad, que se esperaba de los varones a favor de este género. Con el transcurrir del tiempo, esta figura jurídica se hizo extensivo a otros delitos como es, el de comportarse bien, tener ética, valores morales, etc., en cualquier actividad que la persona realiza.

2.2.14.6. Teoría de las subculturas criminales. De acuerdo a Baratta y Silverrnagl (1985) existe una relación de reciprocidad y compatibilidad entre la teoría funcionalista y la teoría de las subculturas criminales. La primera estudia la relación funcional del comportamiento desviado con la estructura social, el plano sobre el que se desarrolla la teoría de las subculturas criminales "tal como se presenta desde sus primeras formulaciones por obra de Shaw y de Thasher hasta Sutherrland, se preocupan sobre todo de estudiar el modo como la subcultura delictiva se comunica a los delincuentes y deja por tanto sin resolver el problema estructural del origen de los modelos subculturales del comportamiento y la comunican que se comunican. Pero desde el momento en que, con la obra de Cohen, el alcance

de las teorías de las subculturas criminales se amplía desde el plano de los fenómenos del aprendizaje subsiste entre las dos teorías un terreno de encuentro, que ha llevado generalmente más de una integración que a una mera compatibilidad" (Peña, 2010).

Existe una integración entre la teoría funcionalista y la teoría de las subculturas criminales. Así lo sostiene Pavarini, cuando afirma que "si se asume que la estructura social de una determinada sociedad ofrecen oportunidades diversas para la consecución de las metas culturales y que esta desigual distribución de los chances de servirse de medios legítimos está en función de la estratificación social, por lo que existen algunos que están siempre y objetivamente excluidos de ella, entonces el método funcionalista de la anomia puede abastecerse de una base explicativa y teórica para la formación de subculturas criminales". La estructura de la sociedad ofrece situaciones importantes, también desaciertos (Paravarini, 1993). Velasco (2010) sostiene que el concepto de subcultura nace en la sociología criminal para explicar la conducta desviada de ciertas minorías; criminalidad de jóvenes y adolescentes de clases bajas organizados en bandas. Respecto a las organizaciones de banda, esta, pues carece de pretensiones generalizadoras. Además, su surgimiento a partir de la década de los cuarenta es tardío, siendo identificado a partir de la obra de Cohen. El presupuesto común de las teorías subculturales es que la delincuencia es una respuesta solución cultural compartida, a los problemas creados por la estructura social (Peña, 2010).

Según Baratta y Silverrnagl (1985) es opinión dominante que a las subculturas corresponden las siguientes características: a) la subcultura es un grupo de rasgos diferentes en relación a la sociedad oficial porque institucionaliza especiales formas de ver el mundo o cosmovisiones; b) su código axiológico o sistema de valores cuenta con cierta autonomía sin llegar a independizarse de la cultura dominante; c) la subcultura tiene una organización interna que regula las relaciones de sus miembros; d) las subculturas surgen en un modelo de sociedad plural y heterogénea. De acuerdo a Garcia (1988) el proceso de interacción con otras personas

que padecen semejante problemas de adaptación social genera un sentimiento de solidaridad de grupo y determinados estándares comunes. Es un mecanismo sustitutivo de participación social y prepara al joven para una carrera criminal de adulto, razón por la cual que todas estas teorías relacionan adolescencia de los delincuentes de clase baja, las bandas y subculturas y carreras delictivas. Estas subculturas también son de aplicación en nuestra realidad nacional

2.2.15. La aplicación del Derecho Penal frente a la utilización de la Inteligencia Artificial/Informática para la perpetración de ilícitos informáticos

El Derecho Penal debe estar continuamente innovándose para efectos de abordar toda la problemática de amenaza que puede llegar a representar el uso indebido de las tecnologías de inteligencia artificial, en cuanto que la manipulación ilegal de tales instrumentos tecnológicos de avanzada por parte de sujetos inescrupulosos que pueden incurrir en la comisión de actos antijurídicos tales como en cuanto a la perpetración de actos delictivos consecuentes relacionados a la sustracción o robo informático de la data informativa privada de personas que resulten vulneradas en sus ámbitos de estricta intimidad personal; como hasta también para darse ejecución de ilícitos agravados como robos y extorsiones con marcaje electrónico - artificial, en que utilizándose aparatos o dispositivos de inteligencia artificial de alta sofisticación electrónica como drones y elementos operativos de última revolución tecnológica 4.0, con los cuales se puede llegar a afectar de manera pluriofensiva a diversos derechos fundamentales de las personas que resulten víctimas de la perpetración de ilícitos derivados del uso ilícito de las tecnologías IA; además de que hasta se puede configurar punitivamente el empleo desnaturalizado de la IA con casos de fines terroristas, lo que de por sí genera la necesidad de que se lleguen a tipificar punitivamente ilícitos que se lleguen a perpetrar de manera específica, que se lleguen a cometer con utilización indebida de la IA, y que implique propiamente que se lleguen a establecer castigos punitivos severos y disuasivos contra los sujetos activos que cometan delitos en base al modus operandi tratado.

Todavía en el Perú, no se ha desarrollado la jurisprudencia vinculante necesaria acerca de procesarse específicamente y condenarse drásticamente a todos aquellos sujetos delictivos que ya vienen empleando determinados instrumentos tecnológicos de Inteligencia Artificial, y que con los cuales se han perpetrado delitos gravísimos, en afectación crítica sobre el patrimonio económico esencialmente de las víctimas vulneradas por actos ilícitos como fraudes y estafas electrónicas, así por otras acciones ilícitas que puedan sufrir por el hackeo de su información económica como personal existente en sus dispositivos móviles de comunicación como en sus redes sociales, y de que los agraviados también lleguen a sufrir la afectación de sus derechos conexos también esenciales como el de resultar dañados en su propia integridad, como en su privacidad e intimidad personal, y hasta inclusive de que puedan sufrir atentados incluso contra su vida por el uso indiscriminado y delincuencial de técnicas de IA de alta peligrosidad para la ciudadanía en general.

En el Perú, el Nuevo Código Procesal Penal, Decreto Legislativo N° 957, en su artículo 207 contempla la implementación de nuevas tecnologías como instrumento para aumentar las posibilidades de éxito en la investigación de los delitos, lo cual se viene desarrollando de manera positiva en los Distritos Judiciales donde dicho instrumento normativo ya está vigente; no obstante, trae consigo algunos problemas legales. Los micrófonos, la masificación de los métodos de captación de sonidos, las video grabaciones, las grabaciones al alcance de cualquier ciudadano han irrumpido muchas veces en la escena penal ocupando un protagonismo que antes carecía, dado que algunas veces resultan invasivas a la intimidad y Dignidad de la persona, convirtiéndose en prueba prohibida, el cual no debe ser valorado por un magistrado si asumimos que estamos en un estado social democrático y de derecho.

Los drones, que en su terminología inglesa drone, o mejor conocido también como aeronave no tripulada (RAE, 2014), han venido revolucionando a la actual sociedad humana, respecto a la ejecución de las funciones de seguridad y vigilancia pública, siempre y cuando se

lleve a cabo, bajo el cumplimiento de las normas y fines debidamente justificables para ello; llegándose así a constituir en uno de los instrumentos de la tecnología de ingeniería informática de amplia innovación y sofisticamiento virtual – artificial que está orientando el desarrollo futuro de la humanidad tanto en el mediano plazo y a futuro; por lo que el empleo de los drones debe trascender en su importancia en cuanto de que pueda generar mayores réditos beneficiables y De producir aportes esenciales para una mayor y mejor calidad de vida en los ciudadanos que se pueda reflejar en el aumento de oportunidades de trabajo en función de deberse plenamente a la debida creación y funcionamiento de empresas modernizadas que empleen tal tecnología de IA para las actividades de seguridad, las telecomunicaciones, y para otros rubros relacionados.

Sin embargo, como señala Santa (2019): “la situación de la actual coyuntura realista del pleno Siglo XXI, cada vez más está enfatizando en aclarar demostrativamente que la utilización aplicativa de drones en la actualidad, también implica el riesgo de que su mala utilización o empleo ilegal también puede conllevar a ocasionar serios problemas delictivos y hasta terroristas que pueden colisionar o afectar gravemente a los bienes jurídicos fundamentales, por lo que se deben tipificar y castigar penalmente de forma drástica, teniendo la debida fundamentación dogmática a nivel del Derecho en su Parte General, y de que se contemple la estructura típica – penal de todos los ilícitos perpetrados con IA, bajo el ámbito específico del derecho penal en su parte especial de manera particularizable, teniéndose muy en cuenta que la mala e incorrecta utilización indebida de los artefactos o instrumentos de IA se puedan llegar a convertir en elementos tecnológicos aptos y recurrentes para la perpetración de diversos delitos en sus formas más agravadas” (Santa, s.f.).

2.2.16. Los riesgos e implicancias negativas de la IA para la perpetración de ilícitos que vulneran los Derechos Fundamentales de las Personas

Como ya se ha referido anteriormente, sobre los malos usos que se pueden dar de las herramientas tecnológicas de la Inteligencia Artificial, tal como se viene dando en países desarrollados, tanto en Estados Unidos como en Europa, en que cada vez más grupos criminales han estado amoldando y sofisticando el modus operandi de sus acciones delictivas, no solamente para vulnerar los bienes jurídicos de la intimidad personal y actos privados de los ciudadanos, para después presionarlos ilícitamente con extorsiones o pago de cupos, con amenazas de difundirse imágenes y videos que puedan afectar la dignidad y vida privada–personal de las personas que resulten afectadas al respecto; sino que también se lleguen a cometer actos delincuenciales que atenten contra el patrimonio económico, la integridad, la seguridad y contra la vida misma de los ciudadanos, que puedan resultar víctimas de robos o asaltos, como de atentados selectivos, habiendo sido reglados previamente por instrumentos modernos basados en sistemas inteligentes – artificiales, los cuales conllevan a la consumación de graves ilícitos que pueden afectar a múltiples bienes jurídicos de las personas, y por ende de que se incremente el nivel de inseguridad ciudadana en el país, recrudeciéndose aquello con el mal empleo de tales tecnologías.

2.2.17. Vulneración de principales Bienes Jurídicos por la perpetración de ilícitos comunes con uso de Herramientas Tecnológicas de Inteligencia Artificial

La mala utilización de la Inteligencia Artificial para fines de comisión de ilícitos puede implicar la grave vulneración de derechos fundamentales de los ciudadanos que resulten afectados por la comisión perpetrable de delitos comunes con uso de recursos tecnológicos de I.A.; tendiéndose a generar daños críticos en las personas agraviadas que puedan sufrir ilícitos cotidianos, pero perpetrados con la utilización indebida de medios que funcionan con sistemas artificiales de Inteligencia, que ponen en grave riesgo a sus bienes jurídicos más vitales como

son la vida, integridad, salud y libertad de los ciudadanos que puedan resultar vulnerados potencialmente por ilícitos perpetrados con tales instrumentos tecnológicos modernizados, que hasta se pueden adquirir en mercados negros y que se pueden readaptar ilegalmente para acciones ilícitas de seguimiento clandestino e ilegal de personas que posean una alta capacidad económica o que por disponer de altos recursos económicos al momento, pueden ser víctimas de reglaje electrónico por drones de I.A. programados para la comisión de actividades delincuenciales de rastreo/seguimiento con marcaje electrónico de víctimas que principalmente vayan a realizar transacciones financieras de fuertes sumas de dinero en Entidades Financieras, y que resultan seguidas hasta sus domicilios, bajo filmación seguible de aparato electrónico tipo dron o de mecanismos de I.A., para que tales víctimas lleguen a ser finalmente asaltadas; aprovechando los sujetos delincuentes las ventajas que les pueden proporcionar los drones o instrumentos artificiales de Inteligencia Electrónica, en grabar a detalle y pormenorizadamente todas las actividades de circulación o de movimientos de las personas que van a ser asaltadas en sí, determinándose con precisión sobre el lugar específico en que se van a perpetrar ilícitos de robo sobre las personas que han sido rastreadas electrónicamente; o inclusive de darse seguimiento delictivo respecto a personas que van a ser asesinadas por ajuste de cuentas, aprovechándose el rastreo electrónico que el dron o aparato de sistema electrónico de Inteligencia Artificial puede llegar a brindar en sí, para fijarse el lugar y hora concreta donde se puede llegar a atentar contra la vida de una persona que haya sido reglada electrónicamente de tal forma.

A contraposición, de que los equipos de drones ya se estén utilizando por parte de las Unidades Especializadas Policiales en cuanto para el seguimiento, filmación e intervención sobre delitos que se perpetren de manera flagrante; pero a contraparte se tiene, que los grupos criminales en los países desarrollados y de manera incipiente en algunos países latinoamericanos, ya han venido adaptando a la ejecución sofisticada de su modus operandi

criminal, la aplicación de tecnología informática de avanzada, en cuanto de Inteligencia Artificial, como el empleo de drones para hacer reglaje electrónico directo y en forma constantemente ilegal sobre las acciones transaccionales económicas que se desempeñen principalmente por parte de ciudadanos que van a ser potencialmente asaltados, tras haber sido seguidos indebidamente por equipos delictivos de drones, los que a su vez delimitarán o establecerán el lugar preciso donde los sujetos delincuentes planearán y cometerán el robo correspondiente o algún otro ilícito agravado.

Conforme se pueden emplear indebidamente los drones y otras herramientas tecnológicas de I.A, para la comisión final o subsecuente de delitos comunes y agravados tales como robos y asesinatos por encargo, en que se puedan atentar contra la vida e integridad de personas que resulten regladas electrónicamente bajo sistemas de Inteligencia Artificial; por lo que se tiende a afectar sus bienes jurídicos esenciales tales como y de la siguiente manera:

2.2.17.1. Afectación de la libertad y seguridad personal de los ciudadanos. En cuanto que aquellos llegan a ser muy vulnerados en torno a su seguridad, al ser reglados o seguidos indebidamente bajo drones o instrumentos electrónicos de I.A., que tienden a vulnerar la libertad individual y seguridad personal con que cada sujeto debe desenvolverse normalmente dentro de la sociedad; y que finalmente tras ser seguidos electrónicamente por tales dispositivos, a posteriori las víctimas pueden sufrir asaltos o ser asesinadas selectivamente por ajuste de cuentas; lo que llegará a incrementar muy negativamente el nivel de percepción de inseguridad ciudadana en las personas, al percibir que su libre circulación está siendo transgredida al ser rastreadas permanentemente por un equipo electrónico dron u otro similar, y de que por ende su seguridad pueda estar en riesgo considerablemente, al estar sometidas a un seguimiento ilegal no consentido por las víctimas, de que por lo cual tendrán el temor constante, de que puedan ser afectadas con un ilícito en cualquier momento, de sufrir

críticamente la vulneración de su libre accionar de movilización, por parte del seguimiento ilícito que se le llegue a efectuar con uso de drones empleados para fines criminales.

2.2.17.2. Vulneración de la libertad de desenvolvimiento personal y del libre tránsito. Que viene a consistir en que los derechos de libre desarrollo personal como de circulación movilizable de los ciudadanos se vean afectados, al estar bajo un ilegal seguimiento electrónico de un dron o equipo de Inteligencia Artificial; que se emplee ilícitamente para el indebido rastreo de los lugares en que pernocten las víctimas bajo reglaje, y la filmación no autorizada de todas las actividades y transacciones que cotidianamente lleguen a realizar; siendo que tales operaciones ilegales formarán parte de los actos ilícitos que sujetos delincuentes o bandas criminales pueden perpetrar, manipulando instrumentos tecnológicos de I.A. para dar seguimiento delictivo a sus víctimas, y de cometer subsecuentemente sobre aquellas delitos de robo, y hasta asesinatos por sicariato o actos de cobro de cupos derivados de extorsiones; resultando así sumamente negativo y hasta crítico de que se vulnere la libertad de tránsito de las víctimas ciudadanas, al sentir temor e inseguridad constante de ser rastreadas o seguidas electrónicamente por drones, a cualquier lugar donde se trasladen para realizar esencialmente alguna importante transacción sea primordialmente de naturaleza económica o financiera, y que por ello puedan ser finalmente rastreadas y hasta ubicadas con drones en cualquier lugar o punto de tránsito, para ser asaltadas de manera agravante por bandas o grupos delincuenciales.

2.2.17.3. Afectación del derecho de privacidad en torno al normal desarrollo de las relaciones personales y particulares de los ciudadanos. Consiste en los daños repercusivos que también se perpetren y lleguen a afectar al bien jurídico esencial de los ciudadanos, sobre su derecho a la privacidad en torno a la ejecución de sus actividades personales y transaccionales – económicas, ya que al estar siendo grabados y seguidos ilegalmente por drones, se vulnera la privacidad reservada de las personas en relación con la

ejecución de sus operaciones transaccionales, y peor aún de que tras ser filmadas por el mecanismo de grabación del dron delictivo, ello facilitará a los delincuentes en actuar consecuentemente con la planeación y ejecución posterior de actos delictivos de robos y estafas en perjuicio de las víctimas rastreadas y grabadas ilegalmente con sistemas de Inteligencia Artificial empleados indebidamente; por lo que asimismo se tiende a generar que los daños personales ocasionados a los agraviados en torno a la violación de la reserva privada de sus operaciones transaccionales, por seguimientos y grabaciones ilegales efectuadas por instrumentos tecnológicos de tipo dron utilizados por grupos delincuenciales, siendo que del daño personal que se produce en torno a la privacidad de las personas víctimas agraviadas, también se deriva en que experimenten y afronten daños de carácter económico, patrimonial y moral al respecto.

2.2.17.4. Daños subsecuentes que se producen en torno a los bienes jurídicos de la vida e integridad de las personas víctimas agraviadas por comisión de delitos en su contra, tras ser sometidas a seguimientos con uso de drones o equipos de I.A. Se trata en sí de los daños consecuentes que se producen en aquellas víctimas que sufren mayormente ilícitos de robos con violencia excesiva o asaltos agravados de parte de dos o más delincuentes; ello tras haber sido regladas o seguidas ilícitamente con drones o por otras herramientas tecnológicas de inteligencia artificial; y que dada la facilidad con que tales instrumentos tecnológicos de I.A. pueden permitir facilitablemente en determinar la ubicación o lugar donde se cometerá el respectivo ilícito contra la persona que haya sido ilegalmente reglada por uso de dron o mecanismo de I.A.; y que como efectos consecuentes se tenga que las víctimas agraviadas, al haber sido seguidas clandestinamente por rastreo ilícito de drones, llegando a ser ubicadas e interceptadas bajo seguimiento electrónico de dron, en lugares alejados, e incluso cerca o en torno a sus viviendas, donde los agraviados pueden sufrir finalmente un asalto en forma agravada, en que puedan resaltar afectados subsecuentemente con graves daños a su

integridad por causa de la excesiva violencia con que se llegue a perpetrar la comisión de ilícitos patrimoniales y que sufren las víctimas, en cuanto a robos con extrema violencia o a mano armada, tal como se viene dando frecuentemente.

Muy aparte también se debe considerar los casos en que se pueden perpetrar asesinatos por sicariato o asesinatos selectivos con utilización peligrosa de instrumentos tecnológicos de I.A., sobre todo de drones que se empleen para hacer el seguimiento ilegal de rastreo electrónico sobre personas que van a ser asesinadas por sicarios o por grupos criminales; sirviendo así los drones para los asesinos sicarios, en permitirles dar información constatable sobre todas las ubicaciones o puntos principales en que las víctimas llegan a pernoctar, y así el sujeto criminal pueda determinar qué lugar es el más propicio para cometer el asesinato.

Conforme a las formas en que se puede tender a vulnerar los bienes jurídicos esenciales de las víctimas agraviadas, que sufran comisión de ilícitos, perpetrados con herramientas tecnológicas de Inteligencia Artificial; se tiende a manifestar por lo tanto que se constituye en una agravante delictiva, en cuanto que para perpetrarse ilícitos comunes como hurtos agravados y estafas, así como ilícitos agravados en cuanto a robos agravados, asesinatos por sicariato y extorsiones, se emplee para la perpetración de tales delitos, como medio de apoyo, en cuanto al uso indebido de los instrumentos o recursos tecnológicos de la I.A., en que generalizadamente tales herramientas modernas permiten hacer un ilegal seguimiento y reglaje electrónico sobre las víctimas, para que los sujetos delincuenciales conozcan pormenorizadamente todos los movimientos, puntos de destino y transacciones operativas que realice cotidianamente la víctima, a efectos de determinarse así el lugar y momento en que acometerá la perpetración del correspondiente acto delictivo contra el blanco objetivo que haya sido reglado por un dron utilizado con fines delictivos.

2.3. Marco histórico

La Internet y su influencia en las sociedades contemporáneas trajo consigo la llamada "Sociedad de la Información"; En nuestro país Internet es representada por la Red Científica Peruana, organismo que funciona de manera autónoma, sin ningún tipo de aporte económico foráneo, su objetivo es el intercambio de información y desarrollo de las telecomunicaciones; esta institución en pocos años, ha difundido enormemente su contenido. Internet no es sino un conjunto de redes que se conectan a través de un protocolo común de comunicación que es el TCP/IP (Transfer Control Protocol/Internet Protocol). Dentro de Internet se comprende a la World Wide Web (www o web) que permite que la información de cualquier red interconectada a Internet pueda ser localizada sin importar su ubicación física. El punto de inicio de funcionamiento del Internet radica en que cada computadora resulta identificada a través del numero IP. Los protocolos se expresan a través de números binarios por conveniencia expresados en forma decimal, sin embargo, esta forma de expresión solo resulta adecuada para los técnicos, mas no para el usuario, creándose así los nombres de dominio "domainnames" (Barriuso, 2000).

Los nombres de dominio no son otra cosa que la dirección de Internet consignada en palabras, de forma tal que resulta fácilmente comprensible para el usuario de Internet. El funcionamiento de este sistema de nombres de dominio ("domainnamessystem" DNS) es a través de bases de datos con listas de los nombres de dominio y sus respectivas direcciones IP. El "domainname" se compone de dos elementos uno identificador (ejemplos conocidos "yahoo", "terra", etc) y otro que sirve para hacer referencia al nivel al que pertenecen ("com", "edu", "gob", etc.). La asignación de los nombres de dominio corresponde hoy en dia a "Internet Corporationfor Assigned Names and Numbres" o ICANN, entidad que se encarga de la administración del sistema de nombres de dominio (Barriuso, 2000).

Los dominios se clasifican en: dominio de nivel superior (“Top Level Domains” o TLD) y dominios de segundo, tercer o cuarto nivel. Los TLD comerciales, “org” para organizaciones, etc.), dominios especiales para entidades que cumplen con ciertos requerimientos (“edu” para entidades educativas, “gov-int” para internacionales, etc.) y dominios internacionales o territoriales (“pe” para Perú, “es” para España, “ar” para Argentina, entre otros). La administración de estos ha recaído sobre las entidades que resultaron ser las primeras en cada país en conectarse a Internet (Lara, 1996).

En paralelo, la informática, Derecho y Derecho Informático, no fueron ajenos a este desarrollo, ya en el año 1962, Philippe Dreyfus emplea el término “Informatique” para unificar dos conceptos: “información” “automática”, con lo que se nace una nueva disciplina, esto es, la Informática se convertiría en el método que iba a servir para afrontar las cuestiones propias del Derecho (Rondinel, 1995).

Al respecto es acertada la definición planteada por Perez (1984), para quien la Informática Jurídica; “estudia el tratamiento automatizado de las fuentes de conocimiento jurídico, por lo que su objeto será “la aplicación de la tecnología de la información al derecho”. Sin embargo, la tecnología informática tiene implicancias que van más allá de la mera aplicación en el derecho y que se encontraban relacionadas a su propia regulación, es así como surge el Derecho Informático como la materia jurídica que comprende al conjunto de disposiciones que regulan las nuevas tecnologías de la información y la comunicación, esto es la informática y la telemática.

De acuerdo a Calderón (2000) en este contexto la actual “Sociedad de la Información” y la “desmaterialización” del Derecho, aparecen nuevas tecnologías que propiciaron un verdadero “cambio de paradigmas”, el antiguo paradigma de la escritura sobre papel se ha transformado en paradigma de la información digital. Esta información, que antes de la aparición de la informática y las redes de interconexión se encontraba confinada en bibliotecas,

con la aparición del fenómeno informático ha sido trasladada, de las bibliotecas oscuras y húmedas, a las computadoras y luego a las redes y el internet, generándose un fenómeno tan impresionante. Tal ha sido la repercusión que ha provocado el fenómeno cibernético en el manejo de la información de nuestras sociedades que se ha optado por denominar a nuestra era como la "era de la información" y a nuestra moderna sociedad como la "Sociedad de la Información".

Esto, en el Derecho, tiene repercusiones bastante evidentes y que se relacionan con la denominada "desmaterialización del Derecho". (Trazegnies, 1998). La aparición de las redes de interconexión y el Internet han acelerado dicha desmaterialización, lo que guarda íntima relación con la propia naturaleza del entorno digital, citemos, por ejemplo, el caso de Internet, que sin ser un "lugar" es un "lugar. Y es que por ella circulan grandes cantidades de información digitalizada, de allí que se le conozca como "súper carretera de información", "aldea global" "red de redes", "red de cobertura geográfica mundial", "ciberespacio" acuñado originalmente por Gibson (Rowland, 1998).

Dentro de este fenómeno de nueva incriminación aparecen conductas que vulneran bienes jurídicos no convencionales y a su vez comportamientos que se realizan empleando medios no convencionales para lesionar bienes jurídicos convencionales. Ambos, por lo general, tienen intrínsecas connotaciones tecnológicas, debido a la incidencia que la evolución tecnológica ha tenido en el cambio social, tal como hemos afirmado. El uso generalizado de la red Internet se debe a sus propias características, las mismas que Mayewski ha descrito de manera didáctica, estas son: la facilidad de su uso, su bajo costo, su velocidad, sus capacidades y la ausencia de límites geográficos (Zaffaroni, 1981).

Tal necesidad, generada desde comienzos de década en sociedades altamente informatizadas, se ha trasladado a sociedades como la nuestra, el reflejo de los avances tecnológicos ha tenido gran influjo en el campo de la criminalidad en tanto este nuevo "modus

operandi" permite captar vacíos en el Derecho Penal tradicional, quedando indefensos "los contenidos inmateriales del sistema informático, su integridad, su disponibilidad o su exclusividad (Cafure, 1995).

2.4. Marco filosófico

En el Perú, el cibercrimen debe pensarse a la luz de la tradición filosófica nacional. Salazar (1968/2004) advertía sobre la necesidad de construir una filosofía auténtica, no imitativa, capaz de responder a los problemas concretos de nuestra sociedad. Aplicado al cibercrimen, esto significa que la reflexión filosófica peruana no puede limitarse a replicar marcos europeos o norteamericanos, sino que debe considerar la desigualdad social, la falta de acceso digital y las brechas de seguridad que caracterizan nuestra realidad.

El Cibercrimen, y los elementos sustantivos y procesales, constituyen un campo donde la filosofía, la ética y el derecho convergen para interpretar los desafíos de la sociedad digital contemporánea. No se trata únicamente de un fenómeno técnico o legal, sino de una problemática ontológica, epistemológica y ética que redefine la noción de delito, de sujeto y de justicia en un espacio desmaterializado. Desde la perspectiva ontológica, el cibercrimen puede entenderse como una manifestación de la acción humana mediada por la técnica. Heidegger (1954/1997) advertía que la técnica no es un simple medio, sino un modo de desocultamiento del ser. Bajo esta premisa, el crimen digital no es un acto aislado, sino un modo de existir en el ser-en-la-red, donde la acción del individuo se proyecta en sistemas distribuidos, algoritmos y datos. El criminal deja de ser únicamente un agente físico para convertirse en un ente híbrido, cuyo accionar trasciende las categorías jurídicas tradicionales.

En términos epistemológicos y verdad en el espacio digital, surge el problema de conocer y probar el delito en un contexto donde las huellas son digitales y fácilmente manipulables. Foucault (1975/2002) señalaba que el poder y el conocimiento se articulan en la construcción de discursos de verdad. En el ámbito del cibercrimen, la verdad judicial se

fundamenta en evidencias técnicas, como registros digitales o metadatos, que reemplazan al testimonio humano clásico. Esto genera un debate sobre la legitimidad y suficiencia de la prueba digital como fundamento de verdad jurídica. En el Perú, donde el sistema judicial aún enfrenta problemas de aplicación de criterios sustantivos - procesales y de prueba digital se convierte en un desafío: ¿cómo garantizar su validez en un sistema judicial que todavía arrastra rezagos de desconfianza social?

Aquí cobra vigencia el pensamiento de Miró Quesada (1981), quien enfatizaba que la filosofía debía abrirse a la racionalidad científica sin perder el horizonte ético. Desde esta perspectiva, la epistemología del cibercrimen exige de aspectos procesales que legitime las pruebas digitales bajo criterios universales de objetividad, pero sin olvidar el deber ético de proteger derechos fundamentales como la privacidad y la dignidad humana.

En cuanto a la dimensión ética de cibercrimen aporta un nivel de análisis fundamental. Según Kant (1785/2002), toda acción debe someterse al imperativo categórico: actuar de tal manera que pueda convertirse en elementos sustantivos y procesales de una ley universal. Aplicado al cibercrimen, el robo de identidad, la intrusión en sistemas o el fraude digital son acciones que, si se universalizaran, socavarían la confianza en la sociedad digital. Desde la óptica utilitarista de Mill (1861/2005), el daño generado por los ciberdelitos excede con creces los beneficios individuales, ya que afecta la economía, la seguridad nacional y la cohesión social.

Por otro lado, Jonas (1979/1995) en su “principio de responsabilidad” señala que el ser humano tiene el deber ético de prever y evitar los daños futuros de sus actos tecnológicos. Bajo esta perspectiva, el hacker que vulnera un sistema crítico no solo afecta a una institución particular, sino que puede poner en riesgo la estabilidad de toda una comunidad interconectada. No obstante, en el contexto peruano, la reflexión debe incluir la ética de la responsabilidad social. Salazar (1968/2004) advertía sobre la condición de dependencia cultural y tecnológica

del Perú. Este enfoque obliga a pensar que la lucha contra el cibercrimen no puede desvincularse de políticas inclusivas que reduzcan las brechas digitales y garanticen que la tecnología no se convierta en un instrumento de dominación, sino en un medio para la justicia social.

Ergo en el contexto filosófico del derecho y justicia en la era digital, los aspectos sustantivos y procesales de la ley de Delitos Informáticos (N.º 30096) y su modificatoria la ley (N° 30171) pueden analizarse desde la tensión filosófica entre libertad y seguridad. Hobbes (1651/2010) justificaba el poder del Estado como garante de paz frente al caos del estado de naturaleza. En el ciberespacio, la ausencia de regulación podría derivar en un "estado de naturaleza digital", dominado por la ley del más fuerte o del más hábil técnicamente. Sin embargo, pensadores como Rousseau (1762/2011) y Rawls (1971/2006) advierten que la legislación debe mantener un equilibrio entre seguridad y derechos individuales, evitando que la protección contra el cibercrimen derive en un modelo de vigilancia totalitaria.

De este modo, los elementos sustantivos y procesales de la ley y su modificatoria, no solo constituyen un conjunto de normas positivas, sino que encarna un debate filosófico profundo sobre la legitimidad del poder, la protección de la libertad individual y la responsabilidad social en la era digital.

El cibercrimen, en su complejidad, no puede reducirse a una mera cuestión de ilegalidad técnica, sino que debe ser comprendido como un fenómeno filosófico que replantea categorías clásicas como justicia, verdad, libertad y responsabilidad. Los aspectos sustantivos y procesales en la ley de ciberdelitos se convierten, entonces, en un instrumento que no solo sanciona, sino que redefine la manera en que las sociedades entienden la convivencia digital. Solo una fundamentación filosófica sólida permitirá otorgar legitimidad a las normativas que buscan equilibrar la protección colectiva con el respeto a los derechos individuales en el ciberespacio.

2.5. Bases Legales

2.5.1. Marco Jurídico Nacional

2.5.1.1. Capítulo IV. Delitos informáticos Contra la Intimidad

2.5.1.1.1. Artículo 6. Tráfico ilegal de datos. Según Ley Nº 30096, 2013, art. 6:

El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera, u otra de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

2.5.1.1.2. Artículo 7. Interceptación de datos informáticos. Según Ley Nº 30096, 2013, art. 7

El que, a través de las tecnologías de información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia. La pena privativa de libertad será no menor de ocho años ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacional.

2.5.1.2. Otras figuras delictivas del Código Penal Peruano

2.5.1.2.1. Artículo 181-A.- Explotación sexual comercial infantil y adolescente en ámbito del turismo. Según Ley Nº 29408, 2009, art. 181:

El que promueve, publicita, favorece o facilita el turismo sexual, a través de cualquier

medio (…) electrónico, magnético o a través de internet, con el objeto de ofrecer relaciones sexuales de carácter comercial de personas de 14 y menos de 18 años de edad.

2.5.1.2.2. Artículo 183-A.- Pornografía infantil. Según Ley Nº 28251, 2004, art. 183-A: El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o pública, importa o exporta por cualquier medio incluido el internet, (…) escritos, imágenes visuales o auditivas, (…) de carácter pornográfico, en los cuales se utilice a personas de 14 y menos de 18 años de edad.

2.5.1.2.3. Artículo 247.- Falsificación de documentos. El que hace uso de un documento falso o falsificado, como si fuese legítimo, siempre
que de su uso pueda resultar algún perjuicio. El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios (MINJUS, 2016).

2.5.1.2.4. Artículo 157.- Uso indebido de archivos computarizados.

El que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas, será reprimido con pena privativa de libertad no menor de 1 ni mayor de 4 años (MINJUS, 2016).

2.5.1.2.5. Artículo 217.- Reproducción, difusión, distribución y circulación de obra sin autorización del autor

(…) el que con respecto a una obra, (...) realiza alguno de los siguientes actos sin la autorización previa y escrita del autor o titular de los derechos:

a. La modifique total o parcialmente.
b. La distribuya mediante venta, alquiler o préstamo público.
c. La comunique o difunda públicamente por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho.

d. La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito (MINJUS, 2016).

La pena será no menor de cuatro años ni mayor de ocho y con sesenta a ciento veinte días multa, cuando el agente la reproduzca total o parcialmente, por cualquier medio o procedimiento y si la distribución se realiza mediante venta, alquiler o préstamo al público u otra forma de transferencia de la posesión del soporte que contiene la obra o producción que supere las dos (2) Unidades Impositivas Tributarias, en forma fraccionada, en un solo acto o en diferentes actos de inferior importe cada uno.

2.5.2. Marco Jurídico Internacional

2.5.2.1. Estados Unidos. La legislación destinada a reprimir el delito informático se encuentra bastante dispersa, aunque son dignas de mención el Acta Federal de Abuso informático, de 1994 que modifico el Acta de Fraude y Abuso informático de 1986, "Communications Decrecy Act", declarada inconstitucional por la Corte Suprema y la "Child Online ProtectionAct".

2.5.2.2. España. Se ha optado por intermedio del proceso de reforma del Código Penal de 1995, hacer frente a las emergentes formas de criminalidad a través de referencias expresas en figuras tradicionales. Así tenemos menciones exprofeso a cuestiones informáticas en los delitos de descubrimientos o revelación de secretos, Robo, Estafa, contra los derechos intelectuales y descubrimiento de secreto empresarial.

En el ámbito extrapenal es la LOPD la normativa que regula el tratamiento automatizado de datos y pretende garantizar el honor la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

2.5.2.3. Alemania. El fenómeno informático se inscribe en la legislación penal germana a través de la Segunda Ley contra la Criminalidad económica que incorporo una serie de delitos relacionados al uso indebido de los sistemas informáticos, así aparecen a) el espionaje

informático (art. 202 C.P.), fraude informático (art.263 C.P.), falsedad informática (art.269 C.P.), alteración de datos (art.303-A C.P.), sabotaje informático (art.303-B C.P.) y la utilización indebida de tarjetas de crédito (art. 266-B C.P.)

2.5.2.4. Portugal. La criminalidad informática en dicho país ha sido abordada mediante la Ley 109/92. Esta norma contiene 19 artículos que se aplican subsidiariamente al Código Penal. El legislador portugués no solo ha tipificado los delitos de falsedad informática (art. 4), daños informáticos (art. 5) sabotaje informático (art.6), intrusismo informático (art. 7), intercepción ilegal (art. 8), sino que establece un glosario de términos (art. 2), una cláusula sobre responsabilidad penal de las personas jurídicas (art. 3 y 10) y un conjunto de consecuencias jurídicas y medidas accesorias (art. 11 al 19).

2.5.2.5. Francia. En enero de 1998 se promulgo en Francia la ley N°88-19 sobre Fraude Informático que reprime el intrusismo informático (462-3 y 462-4 C.P.) y falsificación informática (art.462-5 y 462-6 C.P.).

2.5.2.6. Canadá. En Canadá existen una serie de preceptos relacionados a la criminalidad informática: La sección 342.1 del código Penal reprime el acceso no autorizado de ordenadores (unathorizad use of a computer), la sección 430 sanciona el daño a datos informáticos (mischiefto data), asimismo, tenemos la sección 326 que sanciona la sustracción de servicios de telecomunicaciones (theft of telecommunication service), todas estas conductas se encuentran sancionadas con pena de prisión no mayor de 10 años.

2.5.2.7. Austria. A partir de diciembre de 1987, mediante una ley de reforma del Código Penal, se incorporó en dicho país dos tipos penales relacionados a la cuestión informática: el sabotaje informático (art. 126 C.P.) y el fraude informático (art.148 C.P.).

2.5.2.8. Chile. La vecina nación chilena ha sido una de las pioneras en la regulación de los delitos informáticos en nuestra región, ya desde 1993, por medio de la Ley 19,223 se introdujo en el ordenamiento de Chile una serie de delitos cometidos a través de computadoras.

Las conductas punibles son dos básicamente el sabotaje informático (art. 1 y 3 de la Ley N°19,223) y el espionaje informático (art. 2 y 4 de la Ley N°19,223). La figura de intrusismo informático se encuentra subsumida dentro de la definición del delito de espionaje informático. Las penas previstas para dichos delitos serán de presidio menos en su grado medio a |máximo – en delito de sabotaje informático – y de presidio menor en su grado mínimo a medio – en el delito de espionaje informático.

2.5.2.9. Paraguay. El código Penal de Paraguay incluye algunas importantes prescripciones referidas al ámbito informático, así tenemos que se reprimen los delitos de alteración de datos, el sabotaje informático, el fraude por medio de ordenadores y la destrucción o daño de documentos.

2.5.2.10. En otros Países. Aunque es unánime el interés por la problemática de los delitos informáticos, no obstante, a lo afirmado, actualmente se vienen planteando una serie de propuestas siendo las de mayor interés en nuestro país la de México, Colombia, y la Unión Europea.

III. MÉTODO

3.1. Tipo de investigación

3.1.1. Tipo de investigación

Para Sierra (2003) según su finalidad, la investigación social se puede dividir en, básica y aplicada. La primera tiene como finalidad el mejor conocimiento y comprensión de los fenómenos sociales. Se llama básica porque es el fundamento de toda otra investigación. Por el contrario, la investigación social aplicada, busca mejorar la sociedad y resolver sus problemas. Consiste, de aquí su nombre, en la aplicación de los logros de la investigación básica, de la que por tanto depende, a los fines indicados. De los cuatro oficios principales que cumple la investigación, conocer, explicar, prever o predecir y actuar, los dos primeros constituyen el objeto de la investigación básica, y los dos últimos son aplicaciones de ella y, por tanto, entran en el campo de la investigación aplicada. Ambas investigaciones están pues estrechamente vinculadas.

La investigación desarrollada ha sido la básica porque se ha podido conocer a profundidad la relación de incidencia que existe entre la problemática de incidencia de ilícitos del cibercrimen, que no se han podido combatir ni disminuir eficazmente, a causa de que no se han venido ejecutando los principales aspectos tanto sustantivos como procesales sobre los procesos penales / judiciales contra los imputados por tales delitos, que se dieron en el periodo de los años 2017 y 2018, dentro el distrito Judicial de Lima; teniéndose una alta relación significativa de influencia entre las variables señaladas en torno al problema abordado.

3.1.2. Nivel de investigación

El nivel de la investigación fue correlacional, porque se pretende hacer ver o determinar el grado de relación o asociación no causal que tienen las variables de estudio, entre: Aplicación de los aspectos sustantivos como procesales respecto a litigios judiciales sobre imputados por delitos informáticos, y en lo referente a la incidencia de los delitos de cibercrimen. Hernández

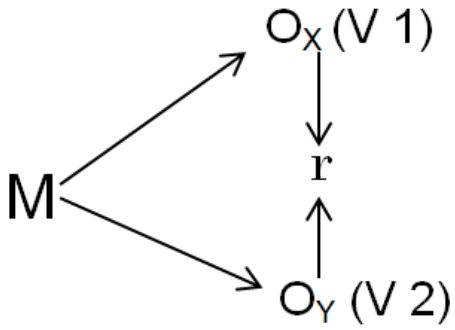
(2010) señala acerca de las investigaciones correlacionales sobre la utilidad y el propósito principal de los estudios correlacionales son saber cómo se pueden comportar un concepto o variable conociendo el comportamiento de otras variables relacionadas. Este estudio mide las dos o más variables que se desea conocer, si están o no relacionadas con el mismo sujeto y así analizar la correlación.

Dado que la investigación se ha basado en el desarrollo de los niveles tanto descriptivo como explicativo, en cuanto que se ha propuesto al mismo tiempo una serie de medidas de corrección que deben tener muy en cuenta los operadores jurídicos - penales para conseguir una plena satisfacción en modo integral de que se puedan mejorar la ejecución de los procesos penales – judiciales contra los denunciados por ilícitos informáticos, y de que estos resulten finalmente sentenciados con condenas punitivas drásticas, como a la vez de sugerirse también en fomentarse una máxima capacitación especializada en todos los operadores jurídicos de derecho penal, que les permitan ejecutar todos los criterios sustantivos de efectiva interpretación de la norma penal que describe todas las conductas punibles de los ilícitos de tipo informático, y en lo que respecta a los criterios procesales que se deben aplicar en función de un desarrollo más agilizable de las etapas de investigación y de juzgamiento de los que resultan imputados por comisión perpetrable de delitos informáticos y en lo concerniente a la protección de todos los bienes jurídicos que se pueden llegar a vulnerar por tales actos delictivos, debiéndose a la carencia o ausencia de una mayor formación tecnológica y pericial en los operadores jurídicos y de justicia penal con respecto a la incidencia de los delitos abordados al respecto.

3.1.3. Diseño de investigación

El diseño que se usó fue No Experimental, descriptivo - correlacional, de acuerdo a la clasificación de Danhker (1989). La investigación tendrá como propósito evaluar la relación

directa que existe entre las variables de estudio, luego describirlo explicando los resultados y representarlos esquemáticamente como:



M= Muestra

Ox, Oy = Observaciones de las variables

r = Relaciones entre las variables

3.2. Población y muestra

3.2.1. Población

La población de estudio estará constituida por el total de Operadores Jurídicos de Derecho Penal (jueces y fiscales adscritos a los juzgados y fiscalías penales) y por el total de Miembros de la Policía Nacional, que vienen desempeñándose en el distrito Judicial de Lima, siendo de un total de 8,550 elementos entre Operadores Jurídicos de Derecho Penal y funcionarios/Efectivos de la Policía Nacional.

3.2.2. Muestra

Según Ruiz (2010) indica que

> La muestra es la parte de la población que se selecciona, de la cual realmente se obtiene la información para el desarrollo del estudio y sobre la cual se efectuarán la medición y la observación de las variables objeto de estudio (p.165).

Para su cálculo se considerará un nivel de error de 5%, 95% de confianza.

Obtención de la muestra:

z = 90% ⇒ 1,65

p = 50% ⇒0,5

q = 1- p ⇒0,5

e = 9 % ⇒0,09

Se consideró la aplicación de la fórmula de cálculo probabilístico de la muestra, en base a la siguiente:

$$\boldsymbol{n = \frac{z^2 Npq}{e^2(N-1) + z^2 pq}} \ldots (\mathbf{1})$$

n = Tamaño de muestra.

z = Desviación de la curva normal

p = Probabilidad de éxito (0.5)

q = 1 – p = 0.5

N = Población

e = 0.09 máximo error permitido

Reemplazando:

$$n = \frac{(1.65)^2(8{,}550)(0.5)(0.5)}{(0.09)^2(8{,}550-1) + (1.65)^2(0.5)(0.5)}$$

$$n = 82\ elementos$$

Teniéndose que la cantidad específica de la muestra de estudio, en cuanto a la muestra definitiva de operadores jurídicos – penales, fue de un tamaño muestral de 82 operadores, repartidos de la siguiente manera estratificada:

Tabla 1

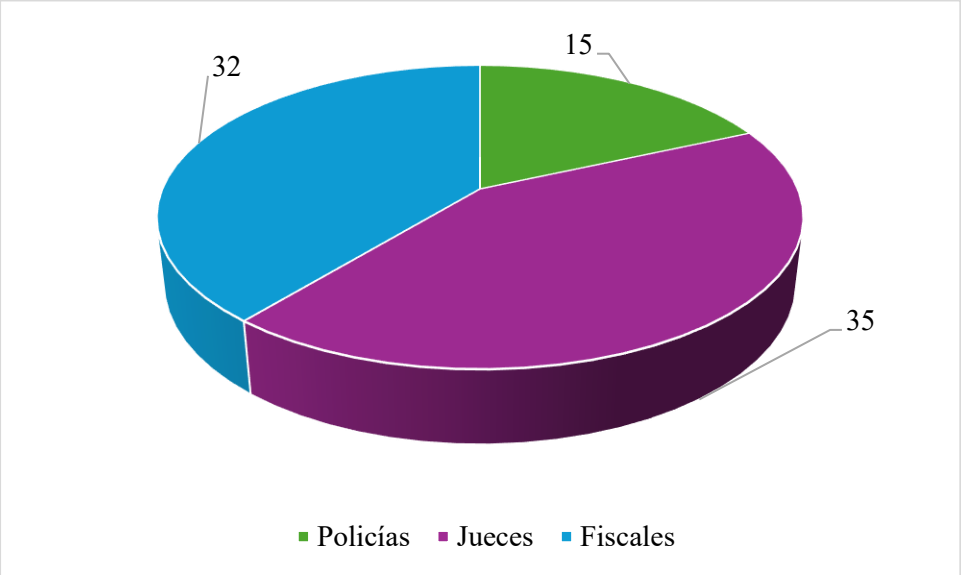
Muestra de estudio

Operadores de Justicia	Total
Policías	15
Jueces	35
Fiscales	32
Total	82

Nota. La muestra estuvo constituida por 82 operadores jurídicos – penales del Distrito Judicial de Lima.

Figura 1

Muestra de estudio



3.3. Operacionalización de variables

Tabla 2

Operacionalización de variables

Dimensiones	Indicadores	N° de Items	Escala y Valores	Niveles	Rango
Problemas en torno a la aplicabilidad de los aspectos sustantivos – penales Se trata del conjunto de vacíos legales y deficiencias que se presentan durante el desarrollo aplicable de determinación de las disposiciones punitivas contenidas principalmente en la Ley N° 30096 del 22/10/2013 modificada por la Ley 30171 del 2014, y del Código Penal vigente, todo ello en relación con la tipificación de los delitos informáticos denunciados y procesados al respecto.	**Vacíos Jurídicos - Penales existentes** • Falta de sanciones punitivas más drásticas para delitos informáticos perpetrados bajo nuevas formas de modus operandi de criminalidad informática. • Carencia de tipicidad penal de modalidades de delitos informáticos que se vienen perpetrándose con el uso de indebido de las redes sociales. • Formas delictivas organizadas para la perpetración de delitos informáticos. • Confusión con lo tipificado entre la Ley Especial y el Código Penal vigente.	1 – 4	Muy de acuerdo (5) De acuerdo (4) Indiferente (3) En desacuerdo (2) Muy en desacuerdo (1)	Bajo Medio Alto	(0 - 8) (9 - 15) (16 - 20)
Problemas durante el desarrollo ejecutable de los aspectos procesales – penales Se refiere a los problemas que se pueden dar por causa de la insuficiencia de métodos y criterios procesales - jurídicos de parte de los Operadores de Derecho Penal, principalmente de los Fiscales y Jueces Penales, al momento respectivamente de imputarse y dictaminarse sentencia condenatoria sobre el delito informático procesado.	**Ausencia de formación tecnológica en delincuencia informática.** • Ausencia de métodos jurídicos efectivos para la imputación de cada delito informático, impide un desarrollo eficaz de su función. • La ausencia de formación tecnológica en delitos informáticos, de los operadores de justicia se encuentra en sintonía con las necesidades de su institución • Mayores facilidades del Estado, en términos de una especialización, de los operadores de justicia	5 - 11	Muy de acuerdo (5) De acuerdo (4) Indiferente (3) En desacuerdo (2)	Bajo Medio Alto	(0 - 8) (9 - 15) (16 - 20)

	sobre delitos informáticos podría favorecer el desarrollo, en su institución • La ausencia de formación tecnológica en delitos informáticos, de los operadores de justicia, incide en la celeridad de sus funciones. • Imposición de penas benignas. • Falta de capacitación en los Jueces Penales sobre la determinación punitiva de los delitos informáticos. • Confusión normativa e interpretativa por las tres leyes procesales penales vigentes (Código Procesal Penal del 2004, Código de Procedimientos Penales de 1940 y Código Procesal Penal de 1991) en el Distrito Judicial de Lima.	Muy en desacuerdo (1)
Problemática en torno a la falta de un mejor desempeño deontológico de los Operadores Jurídicos – Penales en el manejo de la Tecnología Informática, para la investigación y penalización de los delitos informáticos: Consiste en la serie de problemas que llegan a manifestarse en torno a los operadores jurídicos de justicia penal, sobretodo principalmente de Fiscales y Jueces Penales, que no lleguen a conocer o no hacen un buen uso de los medios o herramientas de tecnología informática moderna, como de las comunicaciones modernas en base a las redes sociales; lo que dificulta e impide un efectivo procesamiento judicial – penal sobre los delincuentes informáticos y en cuanto al esclarecimiento de los delitos que perpetren en sí	**Desconocimiento de la Deontología Tecnológica.** • Afectación de la imagen institucional de las Autoridades Competentes, por desconocimiento de la deontología tecnológica de parte de los operadores de justicia. • Afectación de la competitividad en las Autoridades Competentes, por desconocimiento de la deontología tecnológica de parte de los operadores de justicia. • Afectación del desarrollo de calidad de desempeño de las Autoridades Competentes, por desconocimiento de la deontología tecnológica de parte de los operadores de justicia. • Problemática equiparable del desconocimiento de la deontología tecnológica por parte los operadores de justicia en las Autoridades Competentes Peruanas, en relación con las	12-15

	instituciones pares de los países de la región latinoamericana.				
Limitaciones en torno a las propuestas jurídicas. Se tratan de las carencias o ausencias de propuestas jurídicas parlamentarias, del Ejecutivo o particulares, que puedan ser suficientemente pertinentes para mejorarse la efectividad y contundencia en torno a la aplicabilidad de los aspectos sustantivos y procesales que correspondan tanto para una eficaz determinación punitiva y dictaminación competente de sentencias condenatorias drásticas sobre delitos informáticos.	**Transgresiones de las legislaciones vigentes.** • Ausencia de propuestas jurídicas parlamentarias – legislativas más contundentes y completas. • Carencia de propuestas jurídicas legislativas que puedan contemplar reglas procesales - penales específicas para el procesamiento y juzgamiento de delitos informáticos. • Ausencia de propuestas jurídicas del Ejecutivo. • Ausencia de propuestas jurídicas particulares.	16–19	Muy de acuerdo (5) De acuerdo (4) Indiferente (3) En desacuerdo (2) Muy en desacuerdo (1)	Bajo Medio Alto	(0 - 8) (9 - 15) (16 - 20)
Carencia de Recursos de Jurisprudencia Se trata de la insuficiencia y limitaciones en torno a los recursos jurisprudenciales de sentencias judiciales, acuerdos plenarios y resoluciones del Tribunal Constitucional, que puedan hacer referencia más contundente para plantearse soluciones directas a los vacíos legales y problemas existentes en torno a los aspectos sustantivos y procesales para la determinación punitiva de delitos informáticos.	**Insuficiencia Jurisprudencial** • Carencia de sentencias judiciales para la resolución efectiva de casos procesados de delitos informáticos. • Carencia de precedentes judiciales vinculantes. • Carencia de Acuerdos Plenarios para la solución de vacíos legales en torno a aspectos sustantivos de delitos informáticos. • Carencia de Acuerdos Plenarios para la solución de problemas y deficiencias en torno a aspectos procesales de delitos informáticos. • Carencia de resoluciones del Tribunal Constitucional para plantearse soluciones directas a los vacíos legales y problemas existentes en torno a los aspectos sustantivos y procesales para la determinación punitiva de delitos informáticos.	20-24	Muy de acuerdo (5) De acuerdo (4) Indiferente (3) En desacuerdo (2) Muy en desacuerdo (1)	Bajo Medio Alto	(0 - 8) (9 - 15) (16 - 20)

Dimensiones	Indicadores	N° de Items	Escala y Valores	Niveles	Rango
Penalización de Delitos informáticos. Es la configuración punitiva e imposición de las sentencias condenatorias requeridas sobre imputados por la comisión de delitos informáticos.	**Impropia determinación del tipo penal.** • Afectación de la competitividad en la investigación y juzgamiento de los delitos informáticos que hayan vulnerado la intimidad y/o patrimonio de las personas, a causa de la impropia determinación del tipo penal de los ilícitos informáticos correspondientes. • Incidencia negativa de la impropia determinación del tipo penal, en la investigación y juzgamiento de los delitos informáticos que vulneran la intimidad y/o patrimonio de las personas, a causa de que los Fiscales Penales a cargo, no hayan contado con el auxilio de la tecnología informática y jurídica necesaria, para poderse combatir tales ilícitos. • La impropia determinación del tipo penal, llega a redundar en perjuicio de los agraviados, durante la investigación y juzgamiento de los delitos informáticos que se cometieron en perjuicio de su intimidad y/o patrimonio. • La impropia determinación del tipo penal, como desconocimiento de la informática jurídica actualizada en la investigación y juzgamiento de los delitos informáticos que vulneran la intimidad y/o patrimonio de las víctimas. • Falta de Tipicidad Penal completa de todos los delitos informáticos que se pueden perpetrar bajo las nuevas modalidades ilícitas modernas.	25 - 32	Muy de acuerdo (5) De acuerdo (4) Indiferente (3) En desacuerdo (2) Muy en desacuerdo (1)	Bajo Medio Alto	(0 - 8) (9 - 15) (16 -20)

	• Efectiva configuración punitiva sobre delitos informáticos perpetrados en base al uso indebido de las redes sociales. • Vacíos Legales en torno a la tipicidad penal de delitos informáticos contemplados en las Leyes Penales N° 30096 del 2013 y 30171 del 2014. • Vacíos Legales en torno a la tipicidad penal de delitos informáticos contemplados en el Código Penal vigente. **Inadecuada determinación de los daños causados.** • La falta de una adecuada determinación del daño causado a víctimas afectadas en su intimidad y/o patrimonio, se debe a que las Autoridades de Justicia Penal, no llegan a contar con una guía crimino - informática actualizada para favorecerse el desarrollo de las diligencias de investigación y juzgamiento sobre delitos informáticos perpetrados. • La inadecuada determinación de los daños causados, afectan a las víctimas durante y tras el desarrollo ejecutable de las diligencias investigatorias y de juzgamiento sobre todos aquellos delitos informáticos que hayan vulnerado la intimidad y/o patrimonio de las personas dañadas. • La carencia de una adecuada determinación del daño causado, por falta de una preparación más calificada en los operadores de Justicia Penal, en materia de especialidad crimino-informática y asistencia técnica, a su vez no llega a enriquecer y favorecer en la ejecución competente de las acciones diligenciales de investigación y	
Determinación de los daños causados por comisión de ilícitos informáticos Se trata de la capacidad jurídica – penal en que se busca determinar el conjunto de todos los daños que llegan a sufrir las víctimas de delitos informáticos, en cuanto a los daños personales, morales y patrimoniales, que tiendan a experimentar las personas afectadas por la comisión de ilícitos de parte de delincuentes informáticos o por bandas o grupos de cibercriminales.		33-36

	juzgamiento sobre delitos informáticos perpetrados. • Necesidad imperativa de efectuarse los cambios requeridos en el ámbito de desarrollo ejercitable – procesal que maximice la celeridad judicial en la investigación y juzgamiento de los delitos informáticos que hayan vulnerado los bienes jurídicos protegidos de la intimidad y/o patrimonio de las personas afectadas. **Insuficiente cálculo del monto indemnizatorio.** • Necesidad apremiante de una actualización profesional calificada en delitos informáticos, para la reversión del insuficiente cálculo del monto indemnizatorio, en la investigación y juzgamiento de los delitos informáticos que han afectado la intimidad o patrimonio de las víctimas. • Existencia de descontento en la mayoría de los perjudicados respecto al insuficiente cálculo del monto indemnizatorio en la investigación y juzgamiento de los delitos informáticos que han afectado a la intimidad o patrimonio, debiéndose aquello a la falta de credibilidad en la administración de justicia. • Refortalecimiento del papel funcional que le corresponde a las instituciones jurídicas - penales, con relación al ejercitamiento de la función reparatoria en la investigación y juzgamiento de los delitos informáticos que hayan atentado contra la intimidad o patrimonio de las víctimas.	
Determinación del monto indemnizatorio de reparación económica. Viene a consistir en el cálculo determinante del monto de indemnización económica, que deben asumir todos los autores de ilícitos informáticos, en modo de reparación económica a realizarse a sus víctimas afectadas.		37-40

	• Falta de conocimiento de la cifra negra de los delitos informáticos, a causa de la impropia determinación del tipo penal y por la inadecuada determinación del daño irrogado y perjuicio producido en la investigación y juzgamiento de los delitos informáticos que atenten contra la intimidad o patrimonio de las víctimas.				
Disminución de Delitos informáticos. Es el efecto punitivo requerido que implique la reducción drástica de la incidencia comisiva de delitos informáticos, mediante la aplicación de sentencias condenatorias disuasivas al respecto.	**Incidencia Delictiva/Informática** • Reducción progresiva de la incidencia de delitos informáticos. • Disminución efectiva en los últimos dos años. • Disuasión punitiva para prevenirse y evitarse la comisión de delitos informáticos.	41- 43	Muy de acuerdo (5) De acuerdo (4) Indiferente (3) En desacuerdo (2) Muy en desacuerdo (1)	Bajo Medio Alto	(0 - 8) (9 - 15) (16 - 20)

3.4. Instrumentos

Los instrumentos utilizados fueron los cuestionarios que recopilaron datos sobre “el cibercrimen” y “aspectos sustantivos como procesales”.

En lo que respecta a los aspectos sustantivos y procesales del cibercrimen se utilizará un test validado por 3 expertos utilizando la muestra determinada de operadores jurídicos de derecho penal. El instrumento se basará en el cuestionario de encuesta constituido por 09 ítems dirigido a dichos operadores de justicia, para medir el grado de relación entre las variables de estudio establecidas, siendo que las preguntas se han distribuido entre cuatro a seis preguntas referentes a las dimensiones de la variable independiente en base a 24 preguntas, distribuidas acorde con los indicadores como: Los Vacíos Jurídicos - Penales existentes, la Ausencia de formación tecnológica en delitos informáticos, el desconocimiento de la Deontología Tecnológica, las Transgresiones de las legislaciones vigentes, y la Insuficiencia Jurisprudencial; en que la medición se realizó con la escala Likert considerándose cinco categorías o 5 opciones de respuesta, desde Muy de acuerdo (5), De acuerdo (4), Indiferente (3), En desacuerdo (2) y Muy en desacuerdo (1); correlacionado a su vez con los niveles de expectativa de Bajo, Medio y Alto.

Asimismo, para la recopilación de datos de la variable delitos de cibercrimen se utilizó también el instrumento de cuestionario de 09 ítems, constituido por entre tres a ocho preguntas que corresponden a los indicadores de: Impropia determinación del tipo penal, la Inadecuada determinación del daño causado, el Insuficiente cálculo del monto indemnizatorio, y la Incidencia Delictiva/Informática. Se ha aplicado también la escala de Likert con 5 categorías de respuesta, correlacionado a su vez con los niveles de expectativa de Bajo, Medio y Alto.

3.5. Procedimientos

En la presente investigación, se utilizaron las siguientes técnicas:

- Los datos fueron procesados a través de las medidas de tendencia central y de dispersión para presentación de resultados.
- Cuestionario constituido por 43 preguntas dirigido a los operadores jurídicos de derecho penal, para medirse el grado de relación entre el tratamiento de los aspectos sustantivos y procesales por parte de los operadores jurídicos – penales, y el Juzgamiento como Dictaminación de las sentencias contra los autores de delitos informáticos.
- Las hipótesis fueron comprobadas a través del estadístico de coeficiente de correlación de Pearson aplicada a los datos muéstrales.
- En la interpretación de los resultados, la probabilidad con valor menor a 0.05 nos indica que se rechaza la hipótesis nula, caso contrario se acepta la hipótesis alternante.
- En la contratación de la hipótesis se realizó de manera directa teniendo en cuenta los resultados obtenidos en la encuesta, las fuentes de recolección de información utilizada y el aporte del marco teórico como sustento de investigación.
- Fichas bibliográficas y de investigación, para recolectar información sobre los aspectos teóricos de investigación.

3.6. Análisis de datos

Se desarrollaron los cuadros y gráficos estadísticos correspondientes en base a los resultados obtenidos de las encuestas aplicadas a la muestra de 82 operadores jurídicos de derecho penal, habiéndose utilizado para ello el Microsoft Excel Versión Actual; y posteriormente se efectuó la contrastación y validación de las hipótesis de estudio con el software estadístico IBM SPSS Statistic versión 25..

IV. RESULTADOS

4.1. Análisis Descriptivos

El objetivo del presente capítulo es mostrar los diferentes resultados emanados en el estudio concerniente a la relación de influencia que existe entre la aplicabilidad de los aspectos sustantivos como procesales sobre los imputados por la comisión de delitos informáticos, y en lo referente a si se está previniendo, combatiendo y erradicando la incidencia comisiva de delitos del cibercrimen.

Al respecto, Kerlinger (2000) manifiesta que el análisis de los resultados consiste en la categorización, ordenamiento, manipulación y resumen de los datos para obtener respuesta a la pregunta de investigación". Por tanto, los datos procesados e interpretados nos conducirán a constatar la validez o no de la hipótesis de trabajo que ha orientado el desarrollo de la investigación.

En atención a lo señalado se elaboraron una serie de tablas que contienen los resultados fundamentales provenientes del procesamiento de la información con el objeto de dar coherencia a la interpretación de los mismos.

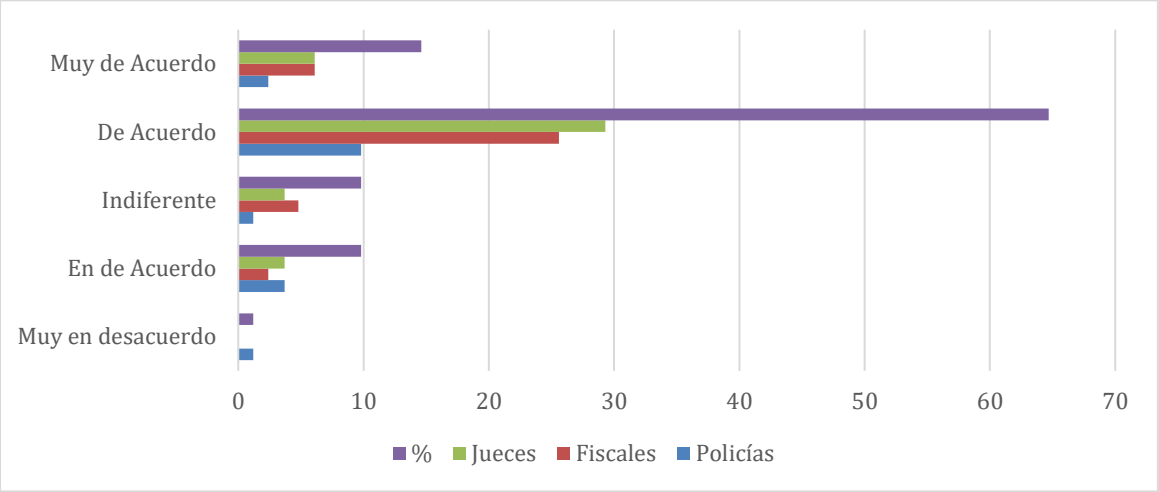
Tabla 3

Vacíos Jurídicos – Penales

Operadores de Justicia	Muy en desacuerdo	En de Acuerdo	Indiferente	De Acuerdo	Muy de Acuerdo
Policías	1.2	3.7	1.2	9.8	2.4
Fiscales	0.0	2.4	4.8	25.6	6.1
Jueces	0.0	3.7	3.7	29.3	6.1
%	1.2	9.8	9.8	64.7	14.6

Figura 2

Niveles de consenso entre Operadores de Justicia



Nota. Existe un consenso generalizado entre los operadores de justicia sobre la existencia de formas delictivas organizadas en la perpetración de delitos informáticos. Este consenso es especialmente fuerte entre jueces y fiscales, quienes probablemente se enfrentan más frecuentemente a casos que evidencian la organización detrás de estos delitos. Sin embargo, las respuestas más variadas entre los policías podrían reflejar diferencias en el nivel de exposición o en la capacitación para identificar estas dinámicas organizadas.

Este análisis resalta la necesidad de fortalecer las capacidades de los operadores de justicia, particularmente los policías, para detectar y combatir estas formas organizadas de criminalidad en el ámbito de los delitos informáticos.

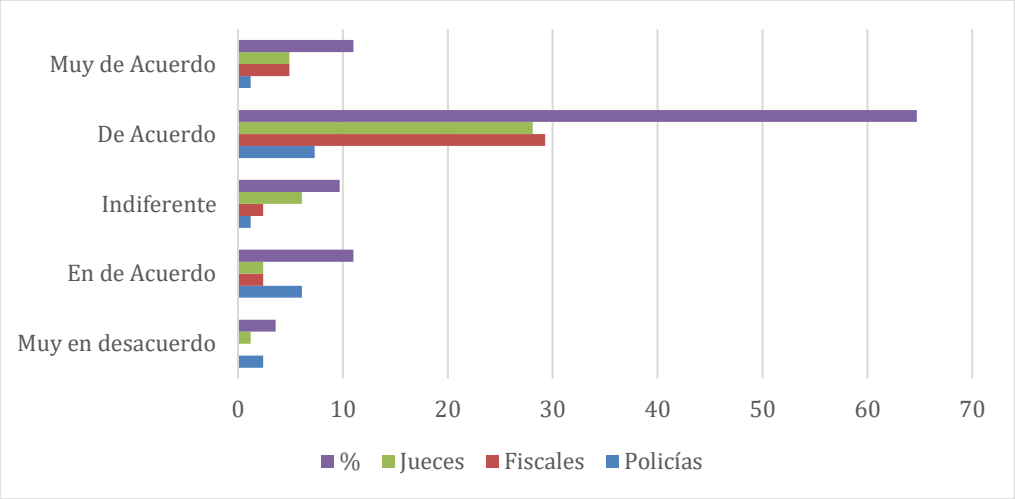
Tabla 4

Ausencia de Formación Tecnológica en Delitos Informáticos.

Operadores de Justicia	Muy en desacuerdo	En de Acuerdo	Indiferente	De Acuerdo	Muy de Acuerdo
Policías	2.4	6.1	1.2	7.3	1.2
Fiscales	0.0	2.4	2.4	29.3	4.9
Jueces	1.2	2.4	6.1	28.1	4.9
%	3.6	11	9.7	64.7	11

Figura 3

Niveles de ausencia de Formación Tca.



Nota. El análisis de los datos muestra que la **ausencia de formación tecnológica en delitos informáticos es percibida mayoritariamente como un obstáculo por los operadores de justicia**. Las diferencias entre los grupos reflejan que fiscales y jueces, debido a la naturaleza de su función, parecen ser más conscientes de la necesidad de esta formación tecnológica. Por otro lado, los policías, aunque también muestran una mayoría de acuerdo, tienen percepciones más variadas. Este consenso sugiere que sería altamente beneficioso implementar **programas de formación tecnológica específicos para todos los operadores de justicia**, con especial énfasis en los policías, para cerrar las brechas de conocimiento y optimizar la gestión de casos relacionados con delitos informáticos.

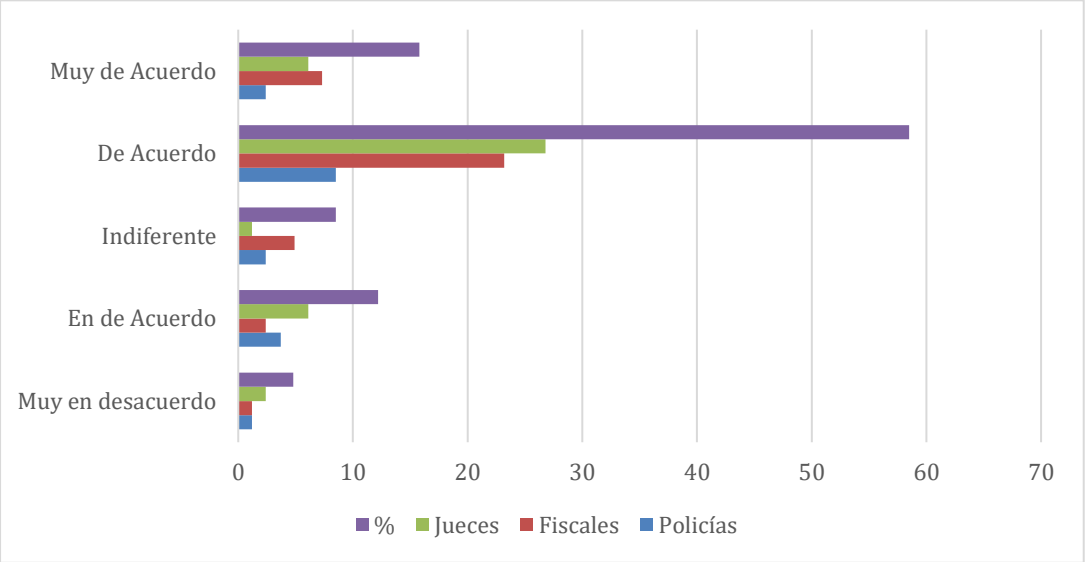
Tabla 5

Transgresiones de las Legislaciones Vigentes

Operadores de Justicia	Muy en desacuerdo	En de Acuerdo	Indiferente	De Acuerdo	Muy de Acuerdo
Policías	1.2	3.7	2.4	8.5	2.4
Fiscales	1.2	2.4	4.9	23.2	7.3
Jueces	2.4	6.1	1.2	26.8	6.1
%	4.8	12.2	8.5	58.5	15.8

Figura 4

Niveles de consenso entre Operadores de Justicia sobre el marco teórico



Nota. Existe un **amplio consenso** entre los operadores de justicia sobre la utilidad de un marco teórico actualizado para delitos informáticos, con más del **74%** de las respuestas totales ubicadas en las categorías "De acuerdo" y "Muy de acuerdo".

Las diferencias entre los grupos reflejan la necesidad de **diseñar y difundir un marco teórico claro y accesible** que facilite la aplicación uniforme de la legislación, evitando transgresiones y mejorando la eficacia en el tratamiento de los delitos informáticos. Los **policías** podrían beneficiarse de una mayor formación y sensibilización sobre la relevancia de este marco teórico.

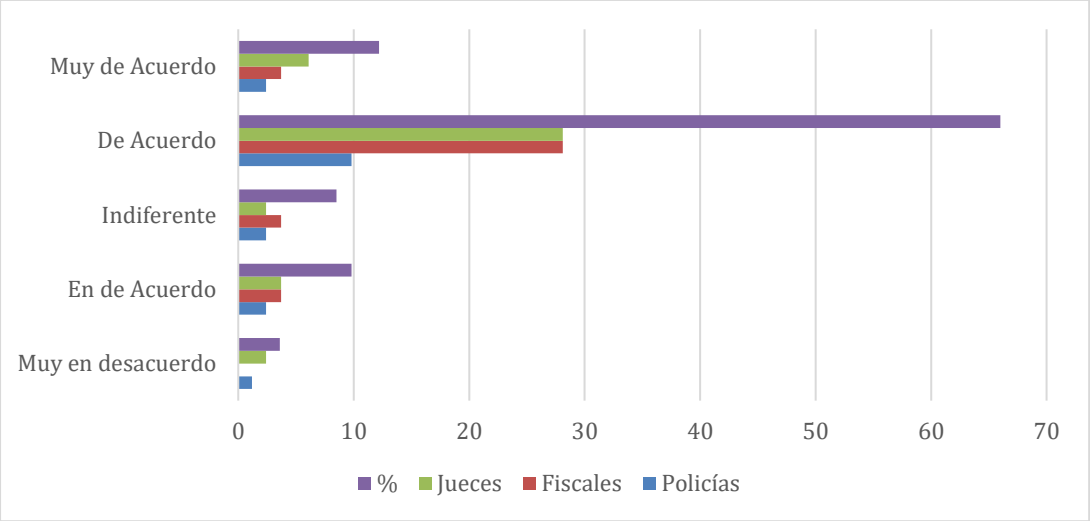
Tabla 6

Insuficiencia Jurisprudencial

Operadores de Justicia	Muy en desacuerdo	En de Acuerdo	Indiferente	De Acuerdo	Muy de Acuerdo
Policías	1.2	2.4	2.4	9.8	2.4
Fiscales	0.0	3.7	3.7	28.1	3.7
Jueces	2.4	3.7	2.4	28.1	6.1
%	3.6	9.8	8.5	66	12.2

Figura 5

Consenso de los Operadores de Justicia para solucionar vacíos legales en Delitos Informáticos



Nota. El análisis refleja un **amplio consenso entre los operadores de justicia sobre la necesidad de acuerdos plenarios para solucionar vacíos legales en delitos informáticos**. Más del 78% de las respuestas están en "De acuerdo" o "Muy de acuerdo", mostrando que esta es una preocupación compartida. La percepción más elevada de acuerdo entre jueces y fiscales resalta su papel crucial en la interpretación de leyes y aplicación de soluciones a estos vacíos legales.

Por otro lado, los policías podrían beneficiarse de una mayor capacitación o concienciación sobre la importancia de estos acuerdos para mejorar su trabajo práctico. Impulsar la creación y difusión de acuerdos plenarios actualizados que aborden los vacíos legales en delitos informáticos, fortaleciendo así la seguridad jurídica y la eficacia en el manejo de estos casos.

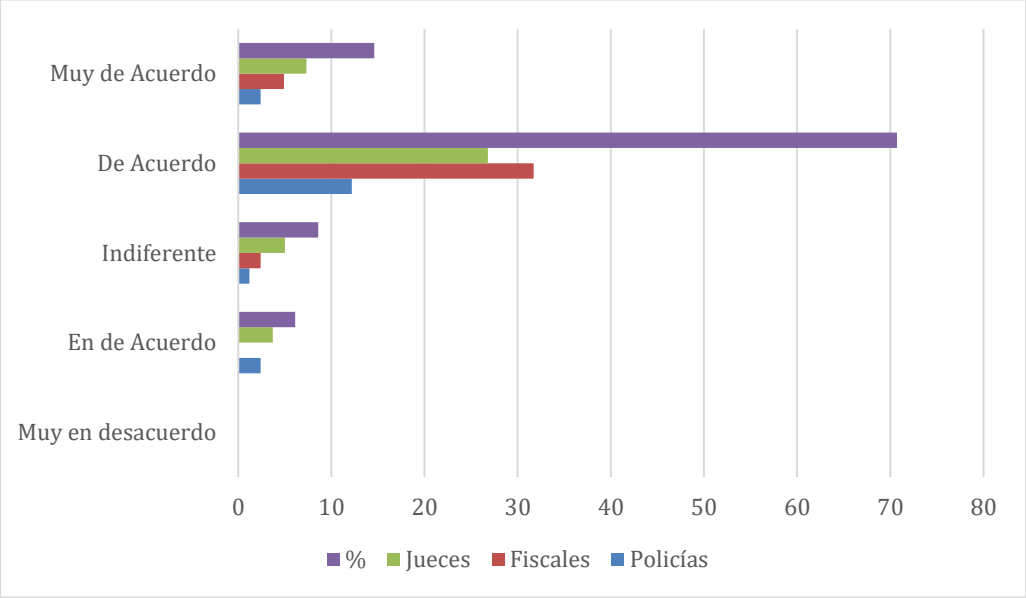
Tabla 7

Valoración impropia determinación del tipo penal

Operadores de Justicia	Muy en desacuerdo	En de Acuerdo	Indiferente	De Acuerdo	Muy de Acuerdo
Policías	0.0	2.4	1.2	12.2	2.4
Fiscales	0.0	0.0	2.4	31.7	4.9
Jueces	0.0	3.7	5.0	26.8	7.3
%	0.0	6.1	8.6	70.7	14.6

Figura 6

Consenso entre Operadores de Justicia para combatir la determinación del tipo penal



Nota. El análisis indica un **amplio consenso entre los operadores de justicia sobre la necesidad del auxilio de la tecnología informática y jurídica para combatir la impropia determinación del tipo penal** en delitos informáticos. Con más del **85%** de las respuestas en las categorías de acuerdo, queda claro que la integración de herramientas tecnológicas es vista como clave para mejorar la investigación y el juzgamiento.

Este resultado subraya la importancia de implementar soluciones tecnológicas que fortalezcan el trabajo de fiscales y jueces, al mismo tiempo que promuevan una mayor sensibilización y

capacitación en su uso para todos los operadores de justicia, incluidos los policías. Esto permitirá abordar los delitos informáticos de manera más precisa y eficaz.

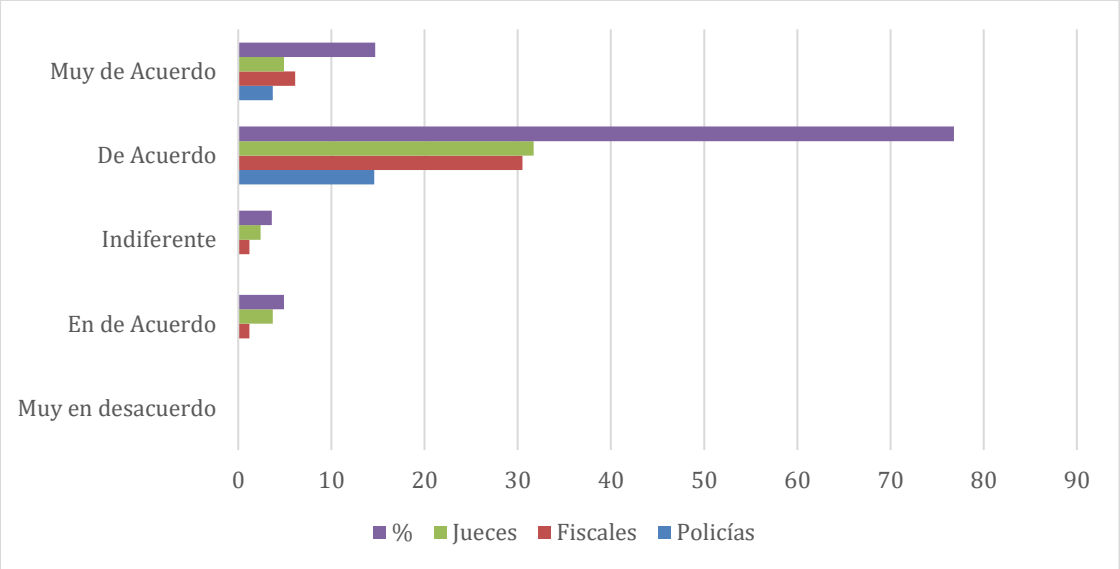
Tabla 8

Inadecuada determinación del daño causado

Operadores de Justicia	Muy en desacuerdo	En de Acuerdo	Indiferente	De Acuerdo	Muy de Acuerdo
Policías	0.0	0.0	0.0	14.6	3.7
Fiscales	0.0	1.2	1.2	30.5	6.1
Jueces	0.0	3.7	2.4	31.7	4.9
%	0.0	4.9	3.6	76.8	14.7

Figura 7

Consenso de los Operadores de Justicia sobre determinación del daño causado.



Nota. El análisis muestra un amplio consenso (91.5%) entre los operadores de justicia sobre el impacto negativo de una inadecuada determinación del daño causado en las víctimas de delitos informáticos. Este consenso refleja la importancia de mejorar los mecanismos y herramientas para determinar el daño en estos casos.

Recomendaciones:

- Implementar protocolos claros y tecnología adecuada para evaluar de manera precisa el daño causado a las víctimas en delitos informáticos.
- Ofrecer capacitaciones específicas a fiscales y jueces para garantizar que la evaluación del daño sea adecuada y que las víctimas reciban justicia plena.
- Sensibilizar a los policías sobre la relevancia de este tema, ya que su rol inicial en la investigación puede ser clave para una correcta determinación del daño.

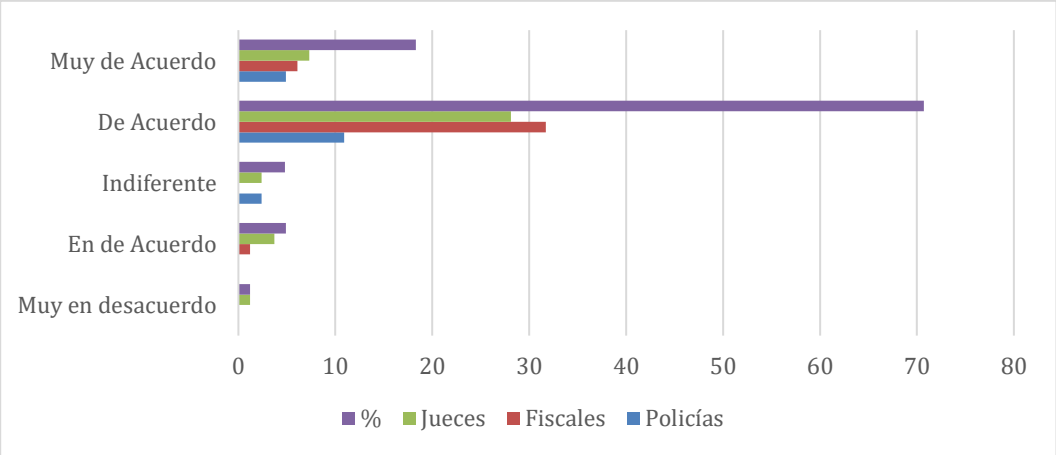
Tabla 9

Insuficiente cálculo del monto indemnizatorio

Operadores de Justicia	Muy en desacuerdo	En de Acuerdo	Indiferente	De Acuerdo	Muy de Acuerdo
Policías	0.0	0.0	2.4	10.9	4.9
Fiscales	0.0	1.2	0.0	31.7	6.1
Jueces	1.2	3.7	2.4	28.1	7.3
%	1.2	4.9	4.8	70.7	18.3

Figura 8

Consenso del (89%) de los Operadores de Justicia sobre insuficiente monto indemnizatorio



Nota. El análisis evidencia un **amplio consenso (89%)** entre los operadores de justicia sobre el descontento de las víctimas respecto al cálculo insuficiente de los montos indemnizatorios y

el impacto negativo que esto tiene en la credibilidad de la administración de justicia. Este resultado subraya la necesidad de una mejora en los procesos de evaluación y determinación de indemnizaciones en delitos informáticos.

Recomendaciones:

- Implementar **protocolos claros y actualizados** para calcular de manera adecuada el monto indemnizatorio en los casos de delitos informáticos.
- Proveer **capacitación especializada** a fiscales y jueces para fortalecer sus capacidades en la determinación justa de las indemnizaciones.
- Sensibilizar a los operadores de justicia, incluidos los policías, sobre la importancia del cálculo justo de indemnizaciones para mejorar la percepción de credibilidad en la administración de justicia.

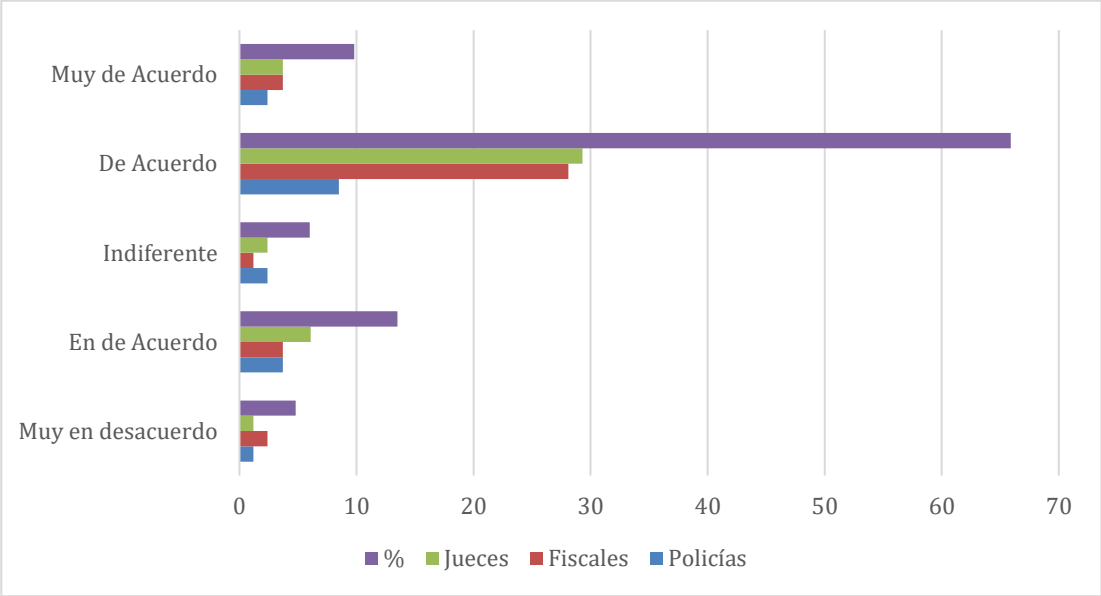
Tabla 10

Incidencia delictiva / informática

Operadores de Justicia	Muy en desacuerdo	En de Acuerdo	Indiferente	De Acuerdo	Muy de Acuerdo
Policías	1.2	3.7	2.4	8.5	2.4
Fiscales	2.4	3.7	1.2	28.1	3.7
Jueces	1.2	6.1	2.4	29.3	3.7
%	4.8	13.5	6	65.9	9.8

Figura 9

Consenso del (75.7%) para prevenir y evitar los Delitos Informáticos



Nota. El análisis muestra un **consenso general (75.7%)** sobre la importancia de la disuasión punitiva para prevenir y evitar la comisión de delitos informáticos. Esto subraya la efectividad percibida de las sanciones penales como un elemento disuasivo en este tipo de criminalidad.

Recomendaciones**:**

- **Fortalecer las sanciones penales** para delitos informáticos, asegurando que sean proporcionales y visibles para aumentar su efecto disuasivo.
- Diseñar programas de **capacitación para operadores de justicia**, con un enfoque en cómo las sanciones efectivas pueden ser utilizadas como herramientas preventivas.
- Aumentar la **concienciación pública** sobre las consecuencias legales de los delitos informáticos para reforzar la percepción de riesgos y prevenir su comisión.

4.1.1. Cuadros y gráficos estadísticos de la variable independiente: Aplicación de los aspectos sustantivos como procesales contra los procesados por delitos informáticos

Tabla 11

Niveles de frecuencia de la variable independiente

Nivel de expectativa	Frecuencia f	Porcentaje %
Bajo	0	0.00
Medio	0	0.00
Alto	82	100.0
Total	82	100

Nota. Se observa que de una muestra de 82 operadores jurídicos penales del distrito Judicial de Lima que representa el 100%, el 100% de los operadores entre Policías, Fiscales y Jueces Penales tienen un nivel alto de opinión acerca de que hay problemas en torno a la aplicación de los aspectos referidos sobre los procesados por delitos informáticos, en el nivel medio y bajo no hubo opinión.

Como podemos observar en los resultados de delitos informáticos en forma general señalamos, que 82 operadores jurídicos de derecho penal (100,0 %) está convencido que hay que trabajar en un mayor establecimiento de los criterios sustantivos como procesales más efectivos al respecto, y que a su vez se garantice plenamente la formación tecnológica en dichos operadores jurídicos.

4.1.2. Cuadros y gráficos estadísticos de la Dimensión 1: Limitaciones en torno a la aplicabilidad de los aspectos sustantivos – penales

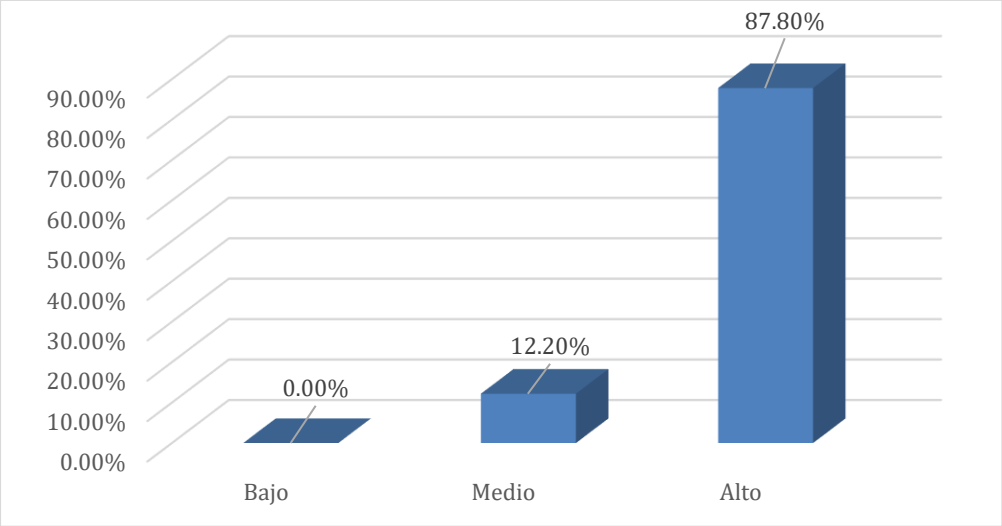
Tabla 12

Tabla de frecuencia de la Dimensión I

Nivel de expectativa	Frecuencia f	Porcentaje %
Bajo	0	0.00%
Medio	10	12.20%
Alto	72	87.80%
Total	82	100%

Figura 10

Niveles de frecuencia de la dimensión 1: Limitaciones en torno a la aplicabilidad de los aspectos sustantivos – penales



Nota. Según los resultados obtenidos (ver cuadro y gráfico) 72 operadores jurídicos (87.80%) del distrito Judicial de Lima, opinan favorablemente acerca que hay Limitaciones en torno a la aplicabilidad de los aspectos sustantivos – penales, 10 operadores (12.20%) opinan media y no hay respuesta para baja.

Como podemos observar en los resultados de la impropia determinación del tipo penal, señalamos, que de 82 operadores jurídicos (100,0 %), el 87.80% está convencido que hay que trabajar en mejorar la aplicabilidad de los aspectos sustantivos - penales, a efectos de mejorarse la inadecuada disposición o señalamiento del tipo penal en relación con el supuesto de hecho, o descripción de la conducta del agente que perpetre un ilícito informático.

4.1.3. Cuadros y gráficos estadísticos de la Dimensión 2: Problemas durante el desarrollo ejecutable de los aspectos procesales – penales

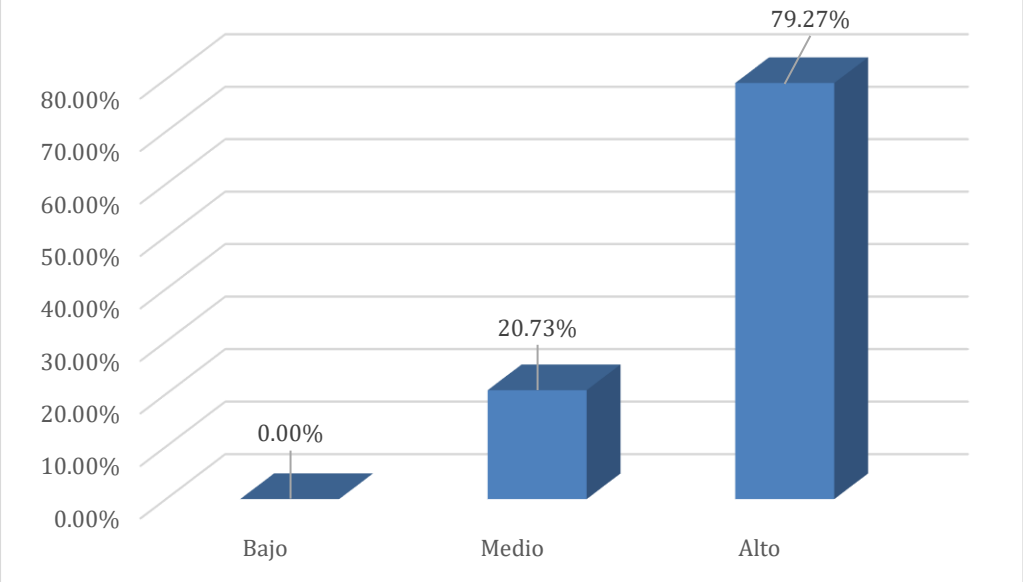
Tabla 13

Tabla de frecuencia de la Dimensión 2

Nivel de expectativa	Frecuencia f	Porcentaje %
Bajo	0	0.00
Medio	17	20,73%
Alto	65	79,27%
-	82	100%

Figura 11

Niveles de frecuencia de la dimensión 2



Nota. Según los resultados obtenidos (ver cuadro y gráfico) 65 operadores jurídicos – penales (79.27%) del distrito Judicial de Lima, opinan favorablemente acerca que hay problemas durante el desarrollo ejecutable de los aspectos procesales – penales, mientras que 17 operadores (20.73%) opinan que es media, y no hay respuesta para la opción de baja.

Como podemos observar en los resultados de la inadecuada aplicación de los aspectos procesales, señalamos, que de 65 operadores jurídicos - penales (79.27%), se refiere a que más

del 50% está convencido de que se deben establecer criterios procesales para mejorarse la ejecución de los procesos litigiosos contra los imputados por tales ilícitos.

4.2. Análisis Inferencial

4.2.1 resultados de la aplicación de los aspectos sustantivos y procesales en torno a los litigios judiciales sobre delitos informáticos y su relación con el combate y erradicación de los delitos de cibercrimen

Test de Normalidad

Para poder aplicar pruebas paramétricas o no paramétricas es necesario comprobar que las variables en estudio tienen o no distribución normal.

La prueba de Kolmogorov-Smirnov (K-S) es aplicada únicamente a variables continuas y calcula la distancia máxima entre la función de distribución empírica de la muestra seleccionada y la teórica, en este caso la normal. Esta prueba es aplicable cuando el número de datos es mayor a 50.

Tabla 14

Prueba de normalidad de las variables

	Kolmogorov-Smirnov[a]		
	Estadístico	**Gl**	**Sig.**
Aspectos Sustantivos y Procesales	,389	82	,000
Delitos de Cibercrimen	,196	82	,000

Para la cual se planteó las siguientes hipótesis:

Ho: El valor calculado es > p=0.05

H_a: El valor calculado es ≤ P=0.05

Decisión:

Según los resultados obtenidos en la prueba K-S, en el instrumento, cuestionario a los operadores, el p valor (Sig) de las variables Aspectos Sustantivos y Procesales sobre los Delitos Informáticos y Juzgamiento como Dictaminación de Sentencias contra los autores por delito de cibercrimen, son menores que 0.05 (0.000), por lo tanto, se acepta la hipótesis alterna (Ha), lo que **significa que no existe normalidad**.

Contrastación de Hipótesis General

Hipótesis Alterna

Ha. Los constantes problemas en el tratamiento aplicable de los aspectos sustantivos y procesales sobre imputados por Delitos Informáticos, influyen negativamente en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, durante los años 2017 – 2018.

Hipótesis Nula

Ho. Los constantes problemas en el tratamiento aplicable de los aspectos sustantivos y procesales sobre imputados por Delitos Informáticos, no influyen negativamente en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, durante los años 2017 – 2018.

- Nivel de significancia: 5%
- Estadístico de prueba:
- Se aplicó la prueba no paramétrica Rho de Spearman.

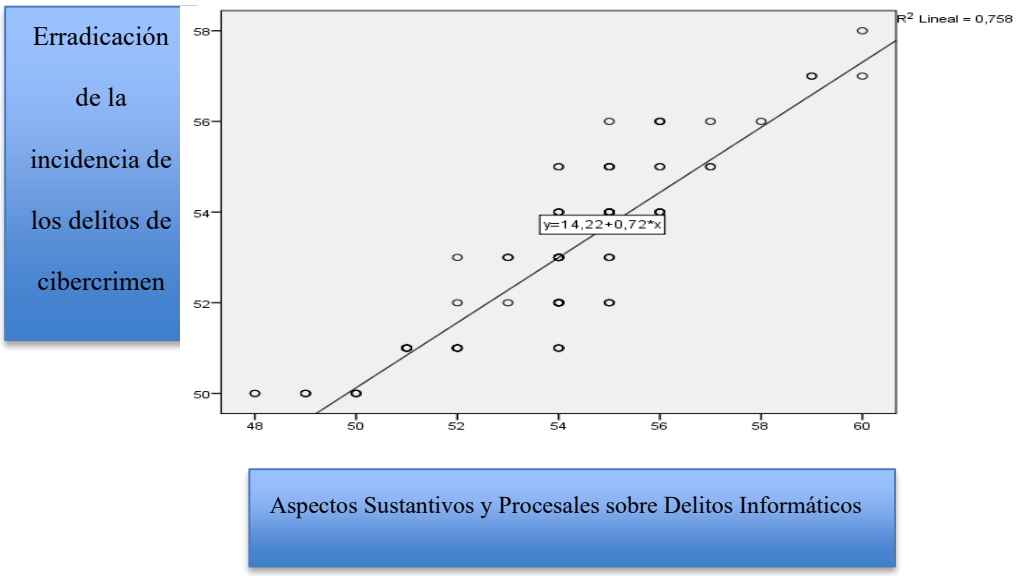
Tabla 15

Prueba Rho de Spearman de la dimensión

			Erradicación de la incidencia de los delitos de cibercrimen
Rho de Spearman	Aspectos Sustantivos y Procesales sobre los Delitos Informáticos	Coeficiente de correlación	,884**
		Sig. (bilateral)	,000
		N	8,550

Figura 12

Dispersión de las variables



Según los resultados obtenidos, el coeficiente de correlación de la Rho de Spearman entre los problemas de falta de aplicabilidad efectiva de los Aspectos Sustantivos y Procesales sobre los Delitos Informáticos, y de no venirse dando la Erradicación de la incidencia de los delitos de cibercrimen; es de 0.884, según la escala establecida, se tiene una correlación de alta influencia al respecto. Además, en el gráfico de dispersión se aprecia que la no disminución de la incidencia criminal de los delitos de cibercrimen se debe a que no se ejecutan como deberían ser los aspectos sustantivos como procesales referentes a los litigios judiciales sobre imputados por delitos informáticos, es decir hay una relación lineal positiva entre las variables graficadas, por lo tanto, es una correlación positiva.

También se muestra el coeficiente de determinación (0.884), es decir, de la falta de una reducción significativa de la incidencia de delitos del cibercrimen, que se predice en torno al 88.4% sobre los casos en que se vienen resolviendo los litigios judiciales sobre imputados por delitos informáticos.

Decisión:

Como p>0,05, se rechaza la Ho

Conclusión:

Según la decisión estadística existe relación significativa positiva entre las carencias y limitaciones de la ejecución aplicativa de los aspectos sustantivos y procesales sobre los imputados por delitos informáticos, con respecto a la falta de disminución sobre la incidencia comisiva de ilícitos del cibercrimen en el distrito judicial de Lima, entre los 2017 y 2018.

4.2.2 resultados de las limitaciones que se presentan en torno al tratamiento aplicable de los aspectos sustantivos – penales de los delitos informáticos, y su influencia con respecto a la penalización y disminución del cibercrimen

Test de Normalidad

Para poder aplicar pruebas paramétricas o no paramétricas es necesario comprobar que las variables en estudio tienen o no distribución normal. La prueba de Kolmogorov-Smirnov (K-S) es aplicada únicamente a variables continuas y calcula la distancia máxima entre la función de distribución empírica de la muestra seleccionada y la teórica, en este caso la normal. Esta prueba es aplicable cuando el número de datos es mayor a 50.

Tabla 16

Prueba de normalidad de la dimensión 2

	Kolmogorov-Smirnov[a]		
	Estadístico	**Gl**	**Sig.**
Delitos Informáticos	,126	82	,000
Impropia determinación del tipo penal.	,331	82	,000

Para la cual se planteó las siguientes hipótesis:

Ho: El valor calculado es > p=0.05

H_a: El valor calculado es ≤ P=0.05

Según los resultados obtenidos en la prueba k-s, en el instrumento, (el cuestionario) a los operadores, el p valor (sig) de las limitaciones que se presentan en torno al tratamiento aplicable de los aspectos sustantivos – penales de los delitos informáticos, y su influencia con respecto a la penalización y disminución del cibercrimen, son menores que 0.05 (0.000), por lo tanto, se acepta la hipótesis alterna (ha), lo que significa que no existe normalidad.

Por lo tanto, se aplicará pruebas no paramétricas, es decir, se aplicará rho de spearman.

V. DISCUSIÓN DE RESULTADOS

En este punto se expondrá una explicación general para los resultados obtenidos en el presente estudio. Además, se discutirán estos hallazgos con los obtenidos en estudios similares con el fin de llegar a una mejor y más ilustrativa interpretación de los mismos. Compararemos los datos obtenidos a través de los instrumentos utilizados en nuestra investigación, es decir, a través del cuestionario cuya escala de medición es categórica ordinal, enfocada a evaluar la actitud de los encuestados.

Se desea saber si es que la aplicación de los aspectos sustantivos y procesales a considerarse en los litigios judiciales sobre imputados por delitos informáticos, llegan a relacionarse con la influencia requerida en la disminución de los ilícitos referidos. La primera variable es respecto a los aspectos sustantivos y procesales aplicables en los litigios judiciales sobre los delitos informáticos, el cual está basado en las siguientes dimensiones:

- Vacíos Jurídicos - Penales existentes.
- Ausencia de formación tecnológica en delincuencia informática.
- Desconocimiento de la Deontología Tecnológica.
- Transgresiones de las legislaciones vigentes.
- Insuficiencia Jurisprudencial.

La segunda variable es sobre los delitos de cibercrimen, el cual está basado en las siguientes dimensiones:

- Impropia determinación del tipo penal.
- Inadecuada determinación del daño causado.
- Insuficiente cálculo del monto indemnizatorio.
- Incidencia Delictiva/Informática

Se evaluó todas las dimensiones esenciales, en lo referente a las limitaciones en torno a la aplicabilidad de los aspectos sustantivos – penales; así como de los problemas durante el

desarrollo ejecutable de los aspectos procesales – penales, y en torno a la Penalización de los Delitos informáticos; siendo que todas estas dimensiones se han cruzado con las variables de estudio tratadas entre sí.

Se encuestó a 82 operadores jurídicos de derecho penal en el distrito Judicial de Lima, dentro del periodo de los años 2017 y 2018.

Conforme a la validación de la hipótesis general de investigación, que se obtuvo con un coeficiente Spearman de 0.884, se concuerda con lo sostenido por Caballa (2015), quien sostiene de que no hay una tipicidad penal ni reglas procesales – penales explícitas para poderse tipificar y sancionar a los delitos informáticos latentes y constantes que se configuren y deriven en base al uso indiscriminado de los medios informáticos brindados por el Internet (caso de Facebook y Redes Sociales), por parte de sujetos inescrupulosos para acceder a información confidencial de personas naturales y de empresas, y ocasionar a posteriori graves daños a la credibilidad y patrimonio económico de las personas afectadas.

Considerándose el modus operandi de los delincuentes informáticos que actúan en forma de red organizada e integrada para asestar ataques cibernéticos a la información almacenada en cuentas bancarias y perfiles almacenados en los sistemas informáticos de empresas, y hasta los que se encuentran dentro de las plataformas de base de datos de las redes sociales, las que al ser accedidas invasiva y fraudulentamente por los hackers, pueden en sí estos obtener toda la información personal y financiera de los usuarios a dichas páginas electrónicas, y así poder realizar ilícitamente en modo consecuente transacciones financieras no autorizadas con sus números de cuenta obtenidos, y hasta de la ejecución de operaciones de hackers-sobornos para llegar a realizar formas de chantajes o hasta de extorsiones a los usuarios titulares, que son amenazados y chantajeados para que no se destruyan sus sistemas de archivos de información que posean, y que hayan resultado hackeados.

En el peor de los casos de que las bandas de ciberdelincuentes operen delictivamente para destruir y obtener información de sistemas de información confidencial y altamente clasificada de Entidades o Instituciones de Defensa y de otras de carácter gubernamental del mismo Estado o de otros países; y que los hackers ciberdelincuentes no resulten identificados de ninguna manera, al haber utilizado para ello diversas cuentas y perfiles electrónicos como usuarios de Facebook o de una Red Social determinada.

Se tiene asimismo que con lo determinado en torno a la validación de la hipótesis principal de esta investigación, también se ha podido reconocer que a causa de otros problemas constantes en función del desacierto del trabajo de los operadores jurídicos penales tanto de los Policías, Fiscales y Jueces Penales durante el desarrollo ejecutable de los procesos de investigación y juzgamiento sobre imputados por comisión de delitos informáticos, no se haya logrado disminuir la incidencia de tales ilícitos, ni muchos menos se haya podido asegurar una mayor protección penal de los bienes jurídicos protegidos de las víctimas que resultaron dañadas por los delitos informáticos perpetrados en su perjuicio, según casos procesados y registrados en el Distrito Judicial de Lima, en que la mayoría de los operadores jurídicos - penales encuestados llegaron a estar de acuerdo con dicha problemática en un 87.80% por parte de los jueces penales, y de los fiscales penales, a la vez que sostienen, de que diversos operadores jurídicos no han llegado a acatar la aplicabilidad de las disposiciones normativas - procesales sobre la ejecución de las fases de investigación y en lo referente a la imputación penal sobre la perpetración de ilícitos informáticos en torno a lo que se ha podido contemplar en relación con la aplicabilidad sustantiva de las leyes penales en vigencia; mientras que llegan a estar en desacuerdo sobre tal problema, solo un 12.20% de entre jueces penales y fiscales encuestados.

La validación de la primera hipótesis específica en base al coeficiente rho Spearman de 0.787, de que las limitaciones basadas en los vacíos legales y deficiencias que se tienden a

presentar en función al tratamiento aplicable de los aspectos sustantivos – penales sobre imputados por delitos informáticos, llegan a influir finalmente de manera negativa sobre el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, durante los años 2017 – 2018; llegándose a concordar lo sostenido con lo fundamentado por Sequeiros (2016), de que la falta de una armonización adecuada entre las diferentes leyes procesales penales que se vienen aplicando actualmente, concretamente en el Distrito Judicial de Lima, en que se tiene tanto la aplicabilidad del Nuevo Código Procesal Penal del 2004 y complementariamente de lo dispuesto por el Código de Procedimientos Penales de 1940 y de algunos artículos del Código Procesal Penal de 1991, todos ellos aplicados de manera generalizada y básicamente integrados en torno para la investigación de los delitos informáticos, lo que resulta tedioso y confundible para diversos jueces penales, que al encontrarse desactualizados en torno a la imposición de las medidas coercitivas - personales necesarias, sobretodo de la prisión preventiva, que suele aplicarse de manera delimitada para imputados de ilícitos informáticos, y que durante el desarrollo de todo proceso penal – judicial, los Fiscales y Jueces Penales tengan dudas y problemas complejos en torno a la configuración punitiva del delito informático que se llegase a procesar, teniéndose el problema crítico permanente de los vacíos legales existentes en el Código Penal y sobretodo en la Ley Especial sobre delitos informáticos, teniéndose ausencias y carencias normativas con relación a la tipicidad de tales ilícitos, y que tales vacíos pese que han sido difícilmente identificados por los operadores de justicia penal, aún no se hayan solucionado por medio de la jurisprudencia penal pertinente, no existiendo precedentes judiciales efectivos al respecto.

A pesar de que se tiene lo dispuesto tipificablemente en la Ley Penal de Delitos Informáticos – Ley 30096 del 22 de octubre de 2013, sobre los diversos tipos de ilícitos informáticos que se pueden perpetrar por los ciberdelincuentes, sean cuando se perpetran en forma individual o hasta en modo colectivo, pero para los que perpetren en forma asociada

estos delitos informáticos tipo sabotaje informático, acceso ilícito a datos informáticos, fraudes informáticos y otros, mediante operaciones perpetradas en forma de organizaciones criminales o de bandas integradas de ciberdelincuentes, las penas que pueden recibir al respecto, los miembros integrantes de grupos criminales, pueden ser de un promedio de entre 3 a 13 años de prisión, pero que en muchos casos no se llegan a hacer efectivas en su totalidad, además de que suelen reducirse dichas penas condenatorias por cuanto que los imputados no presentan antecedentes penales, además de poder acogerse a los beneficios penitenciarios con lo cual pueden disminuir sus penas y cumplir finalmente cierto tiempo limitado o irrisorio en prisión; resultando por lo tanto que no se llega a disuadir drásticamente a los imputados por delitos informáticos, y que la perpetración de tales ilícitos sea permanente, y que los ciberdelincuentes cada vez más emplean técnicas o métodos más sofisticados para perpetrar más delitos informáticos.

Se necesita una mayor penalidad punitiva para los responsables imputables que perpetren modalidades delictivas – informáticas en forma de crimen organizado, tratándose de sujetos hackers que se coluden entre sí y se integran para perpetrar ataques delictivos – informáticos como formas de sabotaje informático, fraudes, robos informáticos a gran escala, o de afectarse el patrimonio de información de las páginas electrónicas de organismos gubernamentales nacionales y extranjeros; considerándose que las actuales penas aplicables para tales imputados al respecto son muy limitadas y benignas.

Tampoco se llega a tipificar de manera más concreta y específica sobre la incidencia comisiva de los delitos informáticos mediante acciones modus operandi u operaciones ilegales de crimen organizado; en cuanto de que se perpetren actos delictivos de sabotaje informático, de acceso ilícito a datos de sistemas informáticos, robos y fraudes informáticos y de la comisión de diferentes modalidades diversificadas de abuso de mecanismos/dispositivos informáticos, perpetrados sistemáticamente por hackers que operan en organizaciones delictivas sofisticadas;

por lo que al no existir una tipicidad punitiva específica al respecto, las penas que se pueden llegar a aplicar a su vez son mínimas o muy benignas; y más aún para aquellos hackers que llegando a obtener información esencial de personas naturales, la cual lleguen a traficar o suministrar dicha información a organizaciones delictivas dedicadas a robos, extorsiones y a secuestros agravados.

En torno a los problemas en los Aspectos Procesales de Investigación, y Procesamiento/Juzgamiento sobre Delitos Informáticos, se tiene que aparte de presentarse limitaciones y deficiencias en los aspectos sustantivos – penales de la legislación penal peruana sobre la tipificación de los delitos informáticos; también se tienen problemas deficitarios procesales a considerar durante el procesamiento/juzgamiento de imputados por tales ilícitos; en que en primer lugar, se tiene el problema de la falta de capacitación en los Jueces y Fiscales Penales que aún tienen muchas dificultades para aplicar con efectividad lo dispuesto en el contenido punitivo de la Ley 30096 del 22 de octubre de 2013 y las modificaciones introducidas por la Ley N° 30171 del 09 de marzo del 2014, implicando que consecuentemente no se lleguen a dictaminar sentencias drásticas ni ejemplares contra los responsables delictivos de ilícitos informáticos; y por otra parte de que los operadores de derecho/justicia penal (principalmente Fiscales Penales) que todavía no dominan la terminología y tecnicismos relacionados con la Informática Forense – Jurídica, asimismo aún no se aplican criterios y técnicas procedimentales más efectivas y acordes con el uso de las tecnologías informáticas para hacerse más eficientes y acelerables los procesos judiciales sobre imputados por delitos informáticos, y en que se pudiese asegurar la imposición de máximas penas drásticas para los culpables imputables de tales ilícitos, lo que resulta muy obstaculizable al tenerse complicaciones y múltiples dificultades en los mismos jueces penales, que de manera confundible y compleja pueden incurrir finalmente en una determinación impropia y errónea de la configuración punitiva del ilícito informático procesado. Además de que no se disponen de precedentes procesales –

judiciales que permitan una resolución procesal más eficaz e inmediata de los juicios sobre imputados por comisión de ilícitos informáticos.

Se valida la segunda hipótesis específica, con un coeficiente rho Spearman de 0.792, en relación de que los problemas de insuficiencia de métodos y criterios procesales – jurídicos, por parte de los Operadores Jurídicos de Derecho Penal, que llegan a presentarse en relación con la falta de un desarrollo aplicativo de los aspectos procesales – penales, que tienden a influir de manera muy negativa con la falta de eficacia en torno al combate y erradicación del cibercrimen dentro del Distrito Judicial de Lima, y de lo que se dió entre los años 2017 – 2018; lo que en sí llega a concordar con el análisis efectuado para conocerse sobre la situación de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos acorde con los aspectos sustantivos y procesales aplicables en los litigios judiciales sobre imputados por tales ilícitos al respecto, se halló que los jueces penales manifestaron mayormente en estar de acuerdo con un 79.27%, de que no se están aplicando los mencionados aspectos en el enjuiciamiento de los imputados por delitos informáticos, a causa de problemas de insuficiencia normativa en la descripción típica – penal de diversos ilícitos informáticos y por la carencia de criterios procesales que dificultan una mayor celeridad en la ejecución de los litigios judiciales pertinentes; como también de no disponerse de criterios jurisprudenciales para una imposición de penas condenatorias severas a los autores delictivos de tales ilícitos, siendo que estos problemas se han reafirmado por los fiscales penales encuestados. Además se concuerda, con lo aportado por Acosta (2012), quien sostuvo que similarmente se da en Ecuador, señalando que una gran mayoría de los Jueces de la Sala Especializada de lo Penal, Miembros del Tribunal y Jueces de Garantías Penales de Cotopaxi, así como los Fiscales y profesionales del derecho en libre ejercicio; si bien tienden a conocer sobre lo que es el delito informático, pero llegan a desconocer el procedimiento aplicativo que hay que seguir en los mismos por no existir la presencia de estas causas en nuestro medio, en su esencia se lo realizó

como ayuda para solucionar los problemas de administración de Justicia Penal, que existe para sancionar este tipo de delitos. Se ha determinado que los encargados de la administración de justicia y profesionales en libre ejercicio, tienen la necesidad de conocer la normativa penal vigente en materia referente a delitos informáticos, para acceder a los beneficios y saber cuáles son las limitantes que la ley impone a los ciudadanos sobre el tema de los delitos informáticos.

Si los jueces están de acuerdo que, con mayores facilidades del Estado, en términos de una especialización, de los operadores de justicia sobre delitos informáticos podría favorecer el desarrollo, de su institución influye en un 79% promedio sobre estar de acuerdo que la inadecuada determinación del tipo penal ocasionado, afecta a la víctima en la investigación y juzgamiento de los delitos informáticos en la protección penal de los que resulten afectados por dichos ilícitos.

Los jueces y fiscales penales asumieron también estar de acuerdo, que los operadores de justicia de sus respectivas instituciones, aún no se encuentran todavía preparados para pronunciarse eficazmente sobre la responsabilidad civil en sede penal, a diferencia de lo que pueden estar para pronunciarse sobre la responsabilidad penal de los sujetos criminales que cometan delitos informáticos; por lo que no pueden determinar las reparaciones civiles – económicas para los afectados por ilícitos informáticos, lo que llega a influir directamente en más del 50% a considerarse respecto a la incidencia del problema referente sobre la impropia determinación del tipo penal, que a su vez tenderá a afectar a la efectividad de ejecución de las diligencias de investigación y juzgamiento sobre los imputados por delitos informáticos, y mucho menos se llega a garantizar la debida protección de las víctimas que resultan vulneradas por tales ilícitos.

VI. CONCLUSIONES

- La verificación de la ausencia de leyes claras, completas sumado a ciertas deficiencias de la gestión en aspectos legales y penales de los delitos informáticos, la complejidad técnica y jurídica que caracteriza a estos delitos cometidos mediante tecnologías digitales, afectan de manera negativa la lucha contra el cibercrimen y genera inseguridad jurídica, limita la eficacia de las sanciones impuestas en el Distrito Judicial de Lima durante los años 2017 al 2018.
- Se detectó que los operadores jurídicos enfrentan serios problemas en la aplicación correcta de los métodos jurídicos y criterios legales en los procesos penales de ciberdelitos. No obstante, los resultados de esta investigación constituyen un aporte para el diseño de propuestas de formulación de mecanismos de intervención práctica, de capacitación y especialización continua para los operadores jurídicos comprometidos en el combate y la eliminación del cibercrimen en el Distrito Judicial de Lima en el periodo 2017-2018.

VII. RECOMENDACIONES

- Se plantea con este estudio, vinculado a los objetivos logrados, afrontar los problemas en torno a la falta de aplicabilidad más eficaz de los aspectos sustantivos y procesales para un mejor procesamiento penal - judicial sobre los delitos informáticos; frente aquello, se necesitan establecer criterios dogmáticos y procesales más específicos que puedan aplicar los operadores jurídicos – penales, para una adecuada comprensión de los diferentes tipos de conducta penal en relación a los ilícitos informáticos que se lleguen a perpetrar; tal como sucede con el estudio de Acosta (2012) en Ecuador que propone directamente la creación de criterios dogmáticos y procesales aplicables que lo diferencia por su carácter propositivo y operativo. y que asimismo puedan los operadores de justicia ordenar y hacer ejecutar los procedimientos como diligencias para hacer más acelerables la ejecución de los litigios judiciales contra los imputados procesados por delitos informáticos, a efectos de que tales imputables puedan recibir la condena requerida de manera drástica y contundente.
- Se brinda a su vez la recomendación que el Poder Legislativo o Congreso de la República pueda sistematizar las propuestas jurídicas del Poder Judicial y del Ministerio Público, para lograr una tipificación penal más completa contra los delitos informáticos sin vacíos jurídicos - penales al respecto, y sin confusiones en la descripción de los tipos penales sobre los diferentes ilícitos informáticos, para evitarse interpretaciones erróneas que pueda implicar finalmente la absolución penal de los imputados por tales delitos o de que reciban penas condenatorias irrisoriamente benignas. Al respecto el estudio de Caballa (2015) sostiene que no se limita a "crear leyes", sino sugerir una articulación técnica entre los poderes del Estado, específicamente entre el Poder Legislativo, el Poder Judicial y el Ministerio Público.
- Se procede a dar a conocimiento que es fundamental de que se promueva el desarrollo de los cursos de capacitación para todos los operadores jurídicos – penales, tanto para los

Fiscales y Jueces Penales que se vienen desempeñando en el distrito judicial de Lima, y que necesitan aplicar los criterios procesales más competentes para efectos de asegurarse que los sujetos imputables por ilícitos informáticos sean castigados severamente, y se pueda disminuir la incidencia de tales delitos. Otros estudios como González & Márquez (2019) abordan la necesidad de capacitación desde un enfoque general o preventivo.

VIII. REFERENCIAS

Abdulai, M. (2016). *Determinantes del miedo a la victimización del crimen de cibernética: un estudio del fraude a la tarjeta de crédito / debito entre estudiantes de la Universidad de Saskatchewan*. [Tesis de Maestría, Universidad de Saskatchewan]. Institutional Repositories. https://n9.cl/w5uqv

Acosta, B. (2012). *Los delitos informáticos y su perjuicio en la sociedad.* [Tesis de Maestría, Universidad Técnica de Cotopaxi]. Repositorio Institucional de la UTC, https://shre.ink/SgFw.

Alanezi, F. (2015). *Las percepciones de fraude en línea y el impacto sobre las contramedidas para el control del fraude en línea en las instituciones financieras de Arabia Saudita.* [Tesis doctoral, Brunel University London]. https://n9.cl/6c153

Alcalá, Z. y Castillo, N. (1985). *Derecho procesal mexicano. S.N.E*. https://n9.cl/nfx8k

Aldama, C. (1993). Los medios informáticos. *Poder Judicial.* (30), 9-26. https://dialnet.unirioja.es/servlet/articulo?codigo=84390

Amoroso, Y. (1991). La informática como objeto de derecho. Algunas consideraciones acerca de la protección jurídica en Cuba de los Datos Automatizados. *Revista Cubana de Derecho.* (1), 43. https://n9.cl/g9wwe3

Aniyar, L. (1980). El delito de cuello blanco en América Latina: Una investigación necesaria. *Ilanud al Día*, *3* (8). 79-81. *https://n9.cl/3qdjj3*

Artega, A. (1987) El delito informático: algunas consideraciones jurídico penales. *Revista de la Facultad de Ciencias Jurídicas y Políticas, 68*(33), 125-133. https://saber.ucv.ve/

Bandler, J., y Merzon, A. (2020). *Cybercrime Investigations: A Comprehensive Resource for Everyone.* CRC Press. *https://doi.org/10.1201/9781003033523*

Baratta, A. (1985). La legislación de emergencia y el pensamiento jurídico garantista en el proceso penal, *Doctrina penal. 8*(32), 559-595. https://biblioteca.csjn.gov.ar/cgi-bin/koha/opac-detail.pl?biblionumber=346530

Barriuso, C. (2000). *Nombres de Dominio (DNS), en Internet, en: Libro de ponencias del VII Congreso Iberoamericano de Derecho e Informática, 32,* VII Congreso Iberoamericano de Derecho e Informática. https://studylib.es/doc/541832/nombres-de-dominio--dns---en-internet

Blossiers, J. (2003). *Criminalidad informática.* Ed. Portocarrero.

Blossiers, J., Sylvia, B. y Calderón G. (2000). *Los delitos informáticos en la banca: El Delito del Milenio y el Código Penal Informático y El Derecho Bancario*. Universidad de Freiburg.

Bramont, L. (2012). Delitos Informáticos. *Revista Peruana de Derecho de la Empresa Derecho Informático y Teleinformática Jurídica,* 51. http://www.asesor.com.pe/teleley/5Bramont-51.pdf

Brenner, S. (2017). *Cybercrime and the law: Challenges, issues, and outcomes*. Routledge.

Cafure, E. (1995). El Delito Informático en la agenda internacional, en cuadernos del departamento del Derecho Penal y Criminología. *Lerner, 1,* 93-100. https://tsjrn.opac.com.ar › pergamo › documento.php

Callegari, L. (1985). Delitos Informáticos y Legislación. *Revista de la Facultad De Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana*. *70*, 115.

Calderón, C. (2000). *El Impacto de la Era Digital en el Derecho.* REDI Nº 21.

Camacho, L. (1987). *Delito Informático.* Gráficas Cóndor.

Congreso de la Republica (2000). *Ley N° 27309: Ley que incorpora los Delitos Informáticos al Código Penal.* http://www.pecert.gob.pe/_normas/delitos/LEY-27309.PDF.

Díaz, J. (2009). *Los derechos humanos ante los nuevos avances científicos y tecnológicos. Genética e internet ante la Constitución.* Tirant lo Blanch.

Díaz, I. (2007). *Delitos que Vulneran la Intimidad de las Personas: Análisis crítico del artículo 161-A del Código Penal Chileno.* Ius et Praxis, *13*(1), 291-314. *https://n9.cl/2ps8j9*

Diccionario de la Real Academia Española (2014). *23ª edición – RAE*.

Espinoza, F. (2000). La firma digital en el Perú a propósito del reglamento de la Ley 27269-Ley de firmas y certificados digitales. *Derecho informático y comercio electrónico*, Fondo Editorial de la UIGV. https://fondoeditorialuigvcuadernos.wordpress.com/contactenos/

Espiñeria & Asociados (2013). *El Delito Informático,* 7 http://www.rzw.com.ar/el-delito-informtico/

Faraldo, P. (2009). Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico. *Tirant lo Blanch.* https://n9.cl/csv6a

Fernández, L. Cabezudo, J., Arenas, M., Herrera, R. y Gastelu, J. (2010). *Diseño de herramientas de control y medidas de prevención para evitar ser víctimas de Delitos Informáticos.* Policía Nacional del Perú.

Fernández, J., Miralles, F., y Millana, L. (2019). *Perfil psicosociológico en el ciberdelincuente.* RICSH, *8*(16), 156-177. https://doi.org/10.23913/ricsh.v8i16.179

Foucault, M. (2002). *Vigilar y castigar. Nacimiento de la prisión. Siglo XXI.*

Fried, Ch. (1968). *Privacy*. *Yale Law Journal*, *77,* 475-493. https://doi.org/10.2307/794941

Gálvez, A., Rojas, C. y Delgado, J. (2011). *Derecho penal. Parte especial*. Jurista Editores.

García, A. (1988). *Manual de Criminología, Introducción y teorías de la criminalidad*.

Garvarino, Á. (1990). Nuevas Normas Jurídicas en Materia Informática. *Revista de la Asociación de Escribanos del Uruguay. 76* (1-6), 68-78. https://n9.cl/gw9guz

Gómez, M. (1994). Los delitos informáticos en el derecho español. Informática y Derecho*: Revista Iberoamericana de Derecho Informático.* (4), 481-496. https://dialnet.unirioja.es/servlet/articulo?codigo=251084

Guibourg, R., Aliende, J. y Campanella, E. (2006). *Manual de Informática jurídica*. Edit Astrea.

Heidegger, M. (1997). La pregunta por la técnica. En Conferencias y artículos. *Revista de Filosofía. 5*(1). *55-79. https://doi.org/10.5354/0718-4360.1958.45002*

Heredia, E. (2013). Política Criminal de los Delitos Informáticos. *SCRIBD. https://shre.ink/SbMd*

Hernández, R. & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education.

Hilgendorf, E. (19939). Gibs es ein "Stratech der Risikogesellschaf, *Neue Zefschtf for Stratrechf (NStZ). 1*, 10-16. **https://shre.ink/Sbxj**

Hobbes, T. (2010). *Leviatán. Fondo de Cultura Económica.*

Jonas, H. (1995). *El principio de responsabilidad: ensayo de una ética para la civilización tecnológica.* Herder Editorial.

Kant, I. (2002). *Fundamentación de la metafísica de las costumbres.* Alianza.

Landa, C., y Velazco, A. (2007). *Constitución Política del Perú.* Fondo Editorial de la Pontificia Universidad Católica del Perú.

Lara, J. (1996) *Manual de Informática y Derecho.* Edit. Ariel.

Lima, M. (1984) Delitos Electrónicos. *Revista Criminalía*,1-6. https://n9.cl/hkg7q

Lujan, J. (2010). *El Contenido Material de los Delitos Informáticos en el Código Penal Peruano. SCRIBD.* https://n9.cl/ox7y4c

Magliona, C. y López, M. (2003). *Delincuencia y Fraude Informático. Derecho Comparado y Ley 19.233.* Editorial Jurídica de Chile.

Mayewski, E. (1997). The Presence of a Web Site as a Constitutionally Permissible Basis for Personal Jurisdiction, *Indiana Law Journal*. *73* (1), Article 6. https://www.repository.law.indiana.edu/ilj/vol73/iss1/6

Mill, J. (2005). El utilitarismo. Alianza.

Mir, S. (1992). *Delincuencia informática.* Ministerio Fiscal.

Miró, F. (1981). *Humanismo científico. Fondo de Cultura Económica*. https://n9.cl/nxy50

Ojeda, J. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *CUAD. CONTAB*. *11*(28), 41-66. http://www.scielo.org.co/pdf/cuco/v11n28/v11n28a03.pdf.

Pavarini, M. (1993). *Control y dominación. Teorías criminológicas burguesas y proyecto hegemónico.* Siglo XXI Editores.

Piattini, G. y Peso, E. (2001). Auditoría informática. Alfaomega RA-MA.

Peña, F. y Alonso, R. (2010). *Derecho penal, Parte especial.* Idemsa.

Pérez, C. (1996). Sociedad de riesgos y reforma penal. *Poder Judicial*, *43*(44), 61-84. https://dialnet.unirioja.es/servlet/articulo?codigo=84580.

Prado, V. (2020). *Delitos informáticos y Derecho Penal en el Perú.* Fondo Editorial de la Pontificia Universidad Católica del Perú.

Puelles, R. (2014). *Luces y sombras en la lucha contra la delincuencia informática en el Perú*. Hiperderecho. https://n9.cl/3angzg

Ramos, M. y García, M. (2024). Delitos relacionados con la ciberdelincuencia en el Código penal español. *Revista Jurídica de la Universidad de León. 12*(31), 129-134. https://doi.org/10.18002/rjule.i12.8578

Rawls, J. (2006*). Teoría de la justicia.* Fondo de Cultura Económica.

Reyna, M. (2002). *Manual de Derecho penal económico. Parte general y especial*. Gaceta Jurídica. https://sbiblio.uandina.edu.pe/cgi-bin/koha/opac-detail.pl?biblionumber=6255

Ribagorda, A. (1996*).* Seguridad de las tecnologías de la información. *Ámbito jurídico de las tecnologías de la información. 11*(1), 307-318. https://dialnet.unirioja.es/servlet/articulo?codigo=552421

Romeo, C. (2013). La penetración del Derecho penal económico en el marco jurídico europeo: los delitos contra los sistemas de información. *Revista brasileira de ciências criminais, 100*, 367-414. https://dialnet.unirioja.es/servlet/articulo?codigo=5067456

Romeo, C. y Flores, F. (2012). *Nuevos instrumentos jurídicos en la lucha contra la delincuencia económica y tecnológica.* Editorial Comares. https://dialnet.unirioja.es/servlet/libro?codigo=543513

Romeo, C. (2006). De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal. *El cibercrimen.* 1-43. Editorial Comares. https://dialnet.unirioja.es/servlet/articulo?codigo=5105395

Rousseau, J. (2011). *El contrato social.* Gredos. https://www.bing.com/search?q=Editorial%20Gredos

Rowland, D. (1998). Cyberspace - A Contemporary Utopia? *The Journal of Information*. http://elj.warwick.ac.uk/jilt/98-3/rowland.html.

Salazar, A. (2004). ¿Existe una filosofía de nuestra América? Fondo Editorial del Congreso del Perú.

Salinas, R. (2006). *Delitos contra el patrimonio.* Jurista Editores.

Salt, M. (1994). *Delitos informáticos de carácter económico.* Editores del Puerto.

San Martín, C. (2018). *Delitos informáticos y derecho penal: Reflexiones sobre la Ley N.º 30096 y su aplicación en el Perú*. Fondo Editorial del Poder Judicial del Perú.

Sánchez, J. (2017). *Adopción de estrategias de Ciberseguridad en la protección de la información en la Oficina de Economía del Ejercito, San Borja 2017*. [Tesis de Maestría, Instituto Científico Tecnológico del Ejército].

Santa, F. (2019). *Drones y Derecho penal. Instituto de Criminología*. UCM. https://n9.cl/houge

Santa, F. y González, F. (2019). *Los drones y la Unión Europea*. UCM. https://shre.ink/Sofc

Sequeiros, I. (2016). *Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo código penal peruano-2015*. [Tesis de maestría, Universidad Hermilio Valdizán de Huánuco]. Repositorio de la UNHEVAL. https://repositorio.unheval.edu.pe/

Silva, J. (2006). *La expansión del Derecho penal. Aspectos de la Política criminal en las sociedades postindustriales.*

Suárez A. (2007). *La estafa informática*. Grupo Editorial Ibañez.

Téllez, J. (2007). *Derecho informático*. McGraw Hill.

Temperini, G. (2014). *Delitos Informáticos en Latinoamérica*: *Un estudio de derecho comparado.* [Tesis doctoral, Universidad Nacional del Litoral] http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf.

Toniatti, R. (1991). Libertad Informática y Derecho a la Protección De Los Datos Personales: Principios de Legislación Comparada. *Revista Vasca de Administración Pública, 29*, 139 -162. https://n9.cl/qa6i5

Trazegnies, F. (1998). La desmaterialización del derecho. Del derecho de pernada al Internet. *THEMIS Revista de Derecho*, (38), 7–14. https://revistas.pucp.edu.pe/index.php/themis/article/view/10306

Urlick B. (1986). Risikogesellschaft auf dem Weg in eine andere. Moderne, Frankfurt. https://www.suhrkamp.de/buch/ulrich-beck-risikogesellschaft-t-9783518113653

Velasco, E. (2010). *Delitos cometidos a través de Internet. Cuestiones procesales*. La Ley – Grupo Wolters Kluwer.

Vera, A. (1996). *Delito e informática: la informática como fuente de delito*. Ed. La Ley,

Villavicencio, F. (2015). Delitos Informáticos en la Ley 30096 y la Modificación de la Ley 30071. *Revista virtual del Centro de Estudios de derecho Penal. 1*, 1-30. https://n9.cl/q0r6rj

Wall, D. (2017). *Cybercrime: The transformation of crime in the information age.* Polity Press.

Wang, Q. (2016). *Estudio comparativo de la ciberdelincuencia en Derecho Penal*: China, Estados Unidos, Inglaterra, Singapur y el Consejo de Europa [Tesis doctoral, Universidad Erasmo de Rotterdam]. Repositorio de EUS https://thesis.eur.nl/

Zaffaroni, R. (1982). Consideraciones político- Criminales sobre la Tutela de los Derechos de Autor. *Revista dos tribunales. 22*, 92-98. https://biblioteca.tra.go.cr/cgi-bin/koha/opac-detail.pl?biblionumber=5020

IX. ANEXOS

Anexo A. Matriz de consistencia

EL CIBERCRIMEN EN EL PERÚ ASPECTOS SUSTANTIVOS Y PROCESALES

Problema	Objetivos	Hipótesis	Variables	Indicadores.	Metodología
Problema general: ¿Cómo el tratamiento aplicable de los aspectos sustantivos y procesales sobre imputados por Delitos Informáticos, viene influyendo en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, periodo 2017 – 2018? **Problemas específicos:** • Qué limitaciones se presentan en torno al tratamiento aplicable de los aspectos sustantivos – penales de los delitos informáticos, y cómo influyen sobre la penalización y disminución del cibercrimen en el Distrito Judicial de Lima, ¿durante los años 2017 - 2018? • ¿Qué problemas se presentan en torno al desarrollo de los aspectos procesales – penales sobre delitos informáticos, y cómo influyen sobre la penalización y disminución del cibercrimen en el Distrito Judicial de Lima, durante los años 2017 - 2018?	**Objetivo general:** Explicar acerca del tratamiento aplicable de los aspectos sustantivos y procesales sobre imputados por Delitos Informáticos, y cómo viene influyendo en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, periodo 2017 – 2018. **Objetivos específicos:** •Explicar las limitaciones que se presentan en torno al tratamiento aplicable de los aspectos sustantivos – penales de los delitos informáticos, y cómo influyen sobre la penalización y disminución del cibercrimen en el Distrito Judicial de Lima, durante los años 2017 - 2018. Explicar los problemas que se presentan en torno al desarrollo de los aspectos procesales – penales sobre delitos informáticos, y cómo influyen sobre la penalización y disminución del cibercrimen en el Distrito Judicial de Lima, durante los años 2017 - 2018.	**Hipótesis Alterna** H_1 Los constantes problemas en el tratamiento aplicable de los aspectos sustantivos y procesales sobre imputados por Delitos Informáticos, influyen negativamente en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, durante los años 2017 – 2018. **Hipótesis Nula** H_0 Los constantes problemas en el tratamiento aplicable de los aspectos sustantivos y procesales sobre imputados por Delitos Informáticos, no influyen negativamente en el combate y erradicación del cibercrimen, en el Distrito Judicial de Lima, durante los años 2017 – 2018.	**Variable independiente:** X= Tratamiento aplicable de los aspectos sustantivos y procesales por parte de los Operadores de justicia. **Variable dependiente:** Y= Procesamiento y dictaminación de castigos penales sobre Autores de Delitos de Cibercrimen.	• Vacíos Jurídicos - Penales existentes • Ausencia de formación tecnológica en delincuencia informática. • Desconocimiento de la Deontología Tecnológica. • Transgresiones de las legislaciones vigentes. • Insuficiencia Jurisprudencial • Impropia determinación del tipo penal. • Inadecuada determinación del daño causado. • Insuficiente cálculo del monto indemnizatorio. • Incidencia Delictiva / Informática.	**Tipo de investigación:** Básico **Nivel de investigación: Correlacional,** Descriptivo y Explicativo**.** **Población y Muestra** **Población.** Se consideró una población derivada de 8,550 elementos entre Operadores Jurídicos de Derecho Penal y funcionarios de la Policía Nacional, que se vienen desempeñando en función de investigación y esclarecimiento de delitos informáticos en el Distrito Judicial de Lima; a efectos de poderse seleccionar una cantidad muestral significativa al respecto. La cantidad específica de la muestra de estudio, en cuanto a la muestra definitiva de operadores jurídicos – penales, es de un tamaño muestral de 82 operadores, Por lo tanto, la muestra fue conformada por 82 encuestados, de las cuales 35 fueron jueces penales, 32 fiscales penales y 15 policías encuestados en total. . **Técnicas e Instrumentos de Recolección de Datos** Para el recojo de estas informaciones, fue necesario utilizar, entre otras las siguientes técnicas: la encuesta, el análisis de contenidos, observación de la realidad problemática; de los cuales se ha podido obtener información, confiable y segura para la demostración de las hipótesis y cumplimiento de los objetivos del presente trabajo. **Técnicas Estadísticas de Análisis y Procesamiento de Datos** Análisis de correlación, y de validación de las hipótesis de estudio mediante la aplicación del software estadístico SPSS 25.0.

Anexo B. Encuestas

UNIVERSIDAD NACIONAL FEDERICO VILLARREAL
ESCUELA UNIVERSITARIA DE POST GRADO
MAESTRIA EN DERECHO PENAL

Título: "El Cibercrimen en el Perú: Aspectos Sustantivos y Procesales"

La presente encuesta tiene como objetivo explicar la causa que influye en el desacierto del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad, en el Distrito Judicial de Lima. Estimados señores Operadores de Justicia, mucho les agradeceremos responder con la mayor objetividad la presente encuesta. Ello redundará en una investigación veraz que incidirá en nuestro futuro trabajo jurisdiccional.

Marque con una X los criterios según el caso

Datos generales:

Cargo: …….....Sexo: ……..... Edad: ……..

Titular……..Provisional: …… Suplente: ……..… Supernumerario: ……..

VALORACION

1. Muy en desacuerdo 2. En desacuerdo 3. Indiferente 4. De acuerdo 5. Muy de acuerdo

Nº	ITEMS	
VACÍOS JURÍDICOS - PENALES EXISTENTES		
1	¿Existe la Falta de sanciones punitivas más drásticas para delitos informáticos perpetrados bajo nuevas formas de modus operandi de criminalidad informática.?	
2	¿Existe la Carencia de tipicidad penal de modalidades de delitos informáticos que se vienen perpetrando con el uso de indebido de las redes sociales?	
3	¿Existen Formas delictivas organizadas para la perpetración de delitos informáticos?	
4	¿Existe confusión con lo tipificado entre la Ley Especial y el Código Penal vigente?	

AUSENCIA DE FORMACION TECNOLOGICA EN DELITOS INFORMATICOS		
5	¿Está Ud. de acuerdo que la ausencia de formación tecnológica en delitos informáticos, de los operadores de justicia, es un obstáculo para un ejercicio eficiente y eficaz de su función?	
6	¿Está Ud. de acuerdo, que la ausencia de formación tecnológica en delitos informáticos, de los operadores de justicia se encuentra en sintonía con las necesidades de su institución?	
7	¿Esta Ud. de acuerdo, que, con mayores facilidades del estado, en términos de una especialización, de los operadores de justicia sobre delitos informáticos podría favorecer el desarrollo, en su institución?	
8	¿Esta Ud. de acuerdo, que la ausencia de formación tecnológica en delitos informáticos, de los operadores de justicia, incide en la celeridad de sus funciones?	
9	¿Existe imposición de penas benignas, a causa de la ausencia de formación tecnológica en la perpetración de los delitos informáticos?	
10	¿Existe la Falta de capacitación en los Jueces Penales sobre la determinación punitiva de los delitos informáticos?	
11	¿Existe la Confusión normativa e interpretativa por las tres leyes procesales penales vigentes (Código Procesal Penal del 2004, Código de Procedimientos Penales de 1940 y Código Procesal Penal de 1991) en el Distrito Judicial de Lima?	
DESCONOCIMIENTO DE LA TECNOLOGIA DEONTOLOGICA		
12	¿Esta Ud. de acuerdo, que el desconocimiento de la deontología tecnológica, de los operadores de justicia, afecta la imagen de su institución?	
13	¿Está Ud. de acuerdo que el desconocimiento de la deontología tecnológica afecta la competitividad de los operadores de justicia, de su institución que está, bien reconocida?	
14	¿Esta Ud. de acuerdo que el desconocimiento de la deontología tecnológica podría incidir en el desarrollo de calidad, de los operadores de justicia, de su institución?	
15	¿Esta Ud. de acuerdo, que el desconocimiento de la deontología tecnológica, de los operadores de justicia, de su institución es equiparable con las instituciones pares de los países de la región?	
TRANSGRESIONES DE LAS LEGISLACIONES VIGENTES		
16	¿Esta Ud. de acuerdo que la ley especial sobre delitos informáticos vigente, constituye un complemento necesario del ordenamiento ya existente, pero, que ello provoca que se cometan transgresiones a las legislaciones vigentes, por parte de los operadores de justicia?	
17	¿Esta Ud. de acuerdo que los operadores de justicia experimentaron cambios que se produjeron en el funcionamiento de su institución, a partir de la entrada en vigencia de la Ley de delitos informáticos, que se manifestaron en transgresiones a las legislaciones vigentes?	
18	¿Esta Ud. de acuerdo, que los operadores de justicia de su institución se encuentran preparado para pronunciarse eficazmente sobre la responsabilidad civil en sede penal como lo está para pronunciarse sobre la responsabilidad criminal, sin que se produzcan transgresiones a las legislaciones vigentes?	
19	¿Esta Ud. de acuerdo, que sería útil contar con marco teórico actualizado de los delitos informáticos, para los operadores no transgredan las legislaciones vigentes?	
	INSUFICIENCIA JURISPRUDENCIAL	
20	¿Existe carencia de sentencias judiciales para la resolución efectiva de casos procesados de delitos informáticos?	
21	¿Existe Carencia de precedentes judiciales vinculantes?	

22	¿Existe Carencia de Acuerdos Plenarios para la solución de vacíos legales en torno a aspectos sustantivos de delitos informáticos?	
23	¿Existe carencia de Acuerdos Plenarios para la solución de problemas y deficiencias en torno a aspectos procesales de delitos informáticos?	
24	¿Existe carencia de resoluciones del Tribunal Constitucional para plantearse soluciones directas a los vacíos legales y problemas existentes en torno a los aspectos sustantivos y procesales para la determinación punitiva de delitos informáticos?	

VALORACION

1. Muy en desacuerdo 2. En desacuerdo 3. Indiferente 4. De acuerdo 5. Muy de acuerdo

Nº	**ITEMS**	
IMPROPIA DETERMINACION DEL TIPO PENAL		
25	¿Esta Ud. de acuerdo, que la impropia determinación del tipo penal, afecta la competitividad en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	
26	¿Esta Ud. de acuerdo, que si el fiscal, contara con el auxilio de la tecnología informática y jurídica, se podría combatir la impropia determinación del tipo penal, en la investigación y juzgamiento de los delitos informáticos?	
27	¿Esta Ud. de acuerdo, que la impropia determinación del tipo penal, redunda en perjuicio del agraviado en la investigación y juzgamiento de los delitos informáticos?	
28	¿Esta Ud. de acuerdo, que la impropia determinación del tipo penal, representa un desconocimiento de la informática jurídica actualizada en la investigación y juzgamiento de los delitos informáticos?	
29	¿Existe la falta de Tipicidad Penal completa de todos los delitos informáticos que se pueden perpetrar bajo las nuevas modalidades ilícitas modernas?	
30	¿Existe efectiva configuración punitiva sobre delitos informáticos perpetrados en base al uso indebido de las redes sociales??	
31	Existen vacíos Legales en torno a la tipicidad penal de delitos informáticos contemplados en las Leyes Penales N° 30096 del 2013 y 30171 del 2014.?	
32	Existen vacíos Legales en torno a la tipicidad penal de delitos informáticos contemplados en el Código Penal vigente.?	

INADECUADA DETERMINACION DEL DAÑO CAUSADO		
33	¿Esta Ud. de acuerdo, que se cumpliría con una adecuada determinación del daño causado, si su institución contara con una guía crimino informática actualizada para favorecer la investigación y juzgamiento de los delitos informáticos?	
34	¿Esta Ud. de acuerdo que la inadecuada determinación del daño causado, afecta a la víctima en la investigación y juzgamiento de los delitos informáticos?	
35	¿Esta Ud. de acuerdo, que una preparación calificada en crimino informática y asistencia técnica, enriquece y favorece la adecuada determinación del daño causado, en la investigación y juzgamiento de los delitos informáticos?	
36	¿Está Ud. de acuerdo, que se necesitan algunos cambios en su ámbito para poder atender los escases de la celeridad procesal judicial de la investigación y juzgamiento de los delitos informáticos?	
INSUFICIENTE CALCULO DEL MONTO INDEMNIZATORIO		
37	¿Está Ud. de acuerdo, que es apremiante la necesidad de una actualización profesional calificada en delitos informáticos, para revertir el insuficiente cálculo del monto indemnizatorio, en la investigación y juzgamiento de los delitos informáticos?	
38	¿Está Ud. de acuerdo, que existe descontento en la mayoría de los perjudicados respecto al insuficiente cálculo del monto indemnizatorio en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad, por ello la falta de credibilidad en la administración de justicia?	
39	¿Está Ud. de acuerdo, que es serio el papel que le corresponde a su institución, respecto de la función reparatoria en la investigación y juzgamiento de los delitos informáticos?	
40	¿Está Ud. de acuerdo, que la cifra negra de los delitos informáticos no se conoce con certeza, por una impropia determinación del tipo penal y una adecuada determinación del daño irrogado y perjuicio producido en la investigación y juzgamiento de los delitos informáticos?	
INCIDENCIA DELICTIVA / INFORMÁTICA		
41	¿Se da con la Reducción progresiva de la incidencia de delitos informáticos?	
42	¿Se da con la disminución efectiva en los últimos dos años, de la incidencia de delitos informáticos?	
43	¿Se da con la disuasión punitiva para prevenirse y evitarse la comisión de delitos informáticos?	

Anexo C. Validación y confiabilidad de instrumentos

La encuesta fue aplicada previamente mediante una prueba piloto del 10 % y fue validada mediante la prueba de $\alpha_{Cronbach}$, que es una media ponderada de las correlaciones entre las variables que forman parte de la escala y validez con R de Pearson; lo que se pudo calcular a partir de las varianzas ($\alpha_{Cronbach}$), arrojando un $\alpha_{Cronbach}$ de 0.788.

Tabla 17

Estadístico de fiabilidad, Alpha de Cronbach del instrumento

Alfa de Cronbach	N de elementos
0.788	43