FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Análisis del Artículo 8º de la Ley N.º 30171 de los Delitos Informáticos contra el Patrimonio en el Perú

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

ABOGADO

AUTORES:

Camacho Llantoy, Juan Jips (ORCID: 0000-0003-1714-0459)

Figueroa Gonzales, Jhon Bernie (ORCID: 0000-0002-8271-3164)

ASESOR:

Dr. PRIETO CHÁVEZ, Rosas Job (ORCID: 0000-0003-4722-838X)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistema de penas, causa y formas del fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA

Fortalecimiento de la Democracia, Liderazgo y Ciudadanía

LIMA – PERÚ

2022

DEDICATORIA

Dedicamos el presente trabajo a todos nuestros seres queridos, nuestros padres y hermanos que nos apoyaron incondicionalmente en el transcurso de nuestra carrera profesional.

AGRADECIMIENTO

Agradecemos a nuestro asesor, docentes, y a todas las personas que hicieron posible la culminación de nuestra investigación.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación titulada “Análisis del artículo 8º de la ley N.º 30171 de los delitos informáticos contra el patrimonio en el Perú” la cual tiene como objetivos específicos; analizar la eficacia del ordenamiento jurídico y el tratamiento normativo respecto a sus modalidades, de los delitos informáticos contra el patrimonio, así mismo tiene como objetivo general, analizar la intervención del Estado para tratar los delitos informáticos contra el patrimonio.

Para ello se utilizó, como métodos de investigación el enfoque cualitativo, de nivel descriptivo, de tipo básico e interpretativo; buscando explicar, aclarar y entender las cuestiones planteadas en la investigación, esta que a su vez es de diseño analítico, basado en el análisis normativo del marco legal peruano del artículo 8º de la ley N.º 30171. A si mismo hemos utilizado como técnica la entrevista mediante el instrumento, como es la ficha de entrevista, con el fin de poder compilar información de especialistas en el tema a fin de fortalecer nuestra investigación.

En tal sentido concluimos, que la intervención del Estado y la regulación de la norma es poco eficiente, toda vez que en estos tres últimos años se ha generado muchos cambios en nuestra vida social a causa de la pandemia por la COVID 19 y el avance de la tecnología, teniendo en cuenta el informe por la OFAEC. indica se elevó al 42% los delitos informáticos, siendo índice preocupante y exigiendo necesidad de tomar acciones por parte de Estado.

Palabras clave: Delitos informáticos, eficacia normativa, patrimonio, Estado, Ciberespacio.

ABSTRACT

The present investigation entitled "Analysis of article 8 of Law N°. 30171 of computer crimes against heritage in Peru" which has specific objectives; analyze the effectiveness of the legal system and the normative treatment regarding its modalities, of computer crimes against heritage, likewise has as a general objective, analyze the intervention of the State to deal with computer crimes against heritage. For this, the qualitative approach, descriptive level, basic and interpretive type was used as research methods; seeking to explain, clarify and understand the issues raised in the investigation, which in turn is of analytical design, based on the normative analysis of the Peruvian legal framework of article 8 of Law N°. 30171. We have used it as a technique the interview through the instrument, such as the interview sheet, in order to be able to compile information from specialists in the subject in order to strengthen our research.

In this sense, we conclude that the intervention of the State and the regulation of the norm is inefficient, since in these last three years many changes have been generated in our social life due to the COVID 19 pandemic and the advance of technology, taking into account the report by the AFOEC indicates that computer crimes rose to 42%, being a worrying index and demanding the need to take action by the State.

Keywords: Computer crimes, regulatory effectiveness, heritage, State, Cyberspace.

I. INTRODUCCIÓN

La problemática jurídica en la regulación de los delitos informáticos contra el patrimonio señalado en el artículo 8º de la ley N.º 30171. A causa de los avances tanto en medios de comunicación y tecnología, permitieron brindar oportunidades para actos delictivos complejos, siendo los grupos criminales los primeros en tomar ventaja de ello, y nuestra legislación a paso de tortuga generando siempre una diferencia, para poder estar a la par respecto a estas nuevas formas de delinquir; mostrándonos una situación aparentemente incontrolable debido a las grandes proyecciones tecnológicas en estos años y con ello un nuevo campo delictivo que originan temor e inseguridad, no solo a las personas naturales; sino también a organizaciones y Estados, aún mucho más desde el inicio de la pandemia 2019, ya que con el estado de emergencia e inmovilización nacional obligatoria ordenado por nuestro Estado peruano y en la misma situación los distintos países, incluido nuestra sociedad, muchos de nosotros hemos optado por recurrir a los medios informáticos, virtuales y cibernéticos para efectuar nuestras actividades diarias, tales como: el teletrabajo, las transacciones financieras virtuales, compras online, estudios virtuales, etc. entre otros, siendo estos medios un gran punto de intercepción y oportunidad para aquellos que gustan de cometer los distintos delitos informáticos. Pero este tipo de actos rechazados por la sociedad, perjudicando a sus víctimas, obstaculizando en sus avances, puesto que al vincularse en el comercio electrónico se vieron muy afectados; del mismo modo teniendo complicaciones para identificar a quienes cometieron esa clase de delitos.

El INEI manifestó que “los Delitos informáticos en el país, el 95% de los ciberdelitos quedaron impunes y solo el 9% de delitos informáticos fueron denunciados de la totalidad de delitos cometidos”. (INEI, 2019)

El total de presuntos delitos que fueron registrados en las fiscalías provinciales y Mixtas alcanzaron los 9750, siendo un tercio de los delitos ingresados correspondientes a delitos contra el patrimonio (31,0%).

Según clasificación específica de los delitos contra el patrimonio, el 52,7% de las denuncias fueron por hurto y 33,4% por robo; en menor porcentaje fueron por

estafa (3,2%), daños (3,1%) y usurpación (2,1%), y de estos 1937 con un 0.7% delitos informáticos. INEI (2019).

El Sr. Orlando Mendieta quien mantiene el cargo de coronel de la Policía Nacional de Perú, mediante el puesto de jefe de la División de Investigación de Alta Tecnología (DIVINDAT) informó que “Los delitos contra el patrimonio y fraudes informáticos llegaron a 2,097 casos, considerados dentro; los fraudes y transacciones, esto durante el 2019 y esta cantidad aumentó en más de 8**%** al 2018 con 1928 casos” (DIVINDAT, 2019)

La presente investigación se encontró vinculada a una realidad problemática que acontecía en nuestra sociedad, siendo el objeto de un profundo y constante estudio llegando arribar tanto en la doctrina como en casos jurisprudenciales e incluso los foros jurídicos, debido a los efectos negativos que causaron; no tan solo a la sociedad sino también a los mismos afectados y los recursos que el estado empleó ante la insuficiencia de los medios de control para sancionar estas conductas.

Respecto a la formulación del problema hemos buscado analizar el artículo 8º de la ley N.º 30171 de los delitos informáticos contra el patrimonio, y mediante especialistas pudimos comprender las acciones que tomó el gobierno por medio de sus entes estatales ante los hechos que contravinieron la norma, garantizando ,protegiendo y velando por los patrimonios e intereses de los mismos; tratándose de una modalidad que día a día tomó mayor fuerza en los últimos años con la situación de la pandemia e aislamiento, por ello no hemos tenido más opción que adaptarnos al uso de estos medios tecnológicos.

Por medio de nuestro trabajo de investigación hemos planteado el O.G: Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio. O.E.1: Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio. O.E.2: Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus modalidades.

En cuanto al supuesto general; la acción del Estado para afrontar los delitos informáticos contra el patrimonio es poco eficiente, Respecto a los supuestos, el específico uno; el artículo 8º de la ley N.º 30171 carece de eficacia frente a los

delitos informáticos contra el patrimonio y el supuesto especifico dos; El tratamiento normativo en cuanto a las modalidades no se encuentra especificadas como tal en los Delitos informáticos contra el patrimonio.

II. MARCO TEÓRICO

Dimos inicio mediante los antecedentes internacionales**,** donde Mayer (2016) concluyó una investigación que lleva por título elementos criminológicos para el análisis jurídico penal de los delitos informáticos, el cual tuvo como objetivo ;determinar la utilización de redes de cómputo para cometer delitos que causen la afectación a los soportes lógicos del sistema informático, esto con la finalidad es distinguir el entorno relacionado a las consecuencias, el sujeto y el acto cometido, así como los medios. El nivel de investigación fue No Experimental, instrumento de análisis documental y se logró determinar; cuan vulnerables se encontraron las victimas ante dicha situación, fue evidente que el riesgo que esto acarreó fue motivo de preocupación y sensibilidad, de esta manera se evidenció que tan importante fue tomar cartas en el asunto, frente a estos nuevos tipos de delitos asociados al uso y avance de la tecnología.

Por otro lado, Martínez, Murillo y Sánchez (2020) concluyó, una investigación que lleva por título desafío del sistema penal salvadoreños en la ejecución de la ley especial frente a los delitos informáticos y asociados, tuvo como objetivo descubrir los inconvenientes posibles en el sistema penal salvadoreño ante el tratamiento y aplicación frente a los delitos informáticos, con la finalidad de conocer que procedimientos debieron ser los adecuados y analizar cada criterio que debió ser considerado por los juristas quienes aplicaran el derecho frente a posibles vacíos e inconvenientes de investigación en un proceso delictivo. El nivel de investigación fue no experimental, mediante análisis documental, instrumento; entrevistas, estudio de casos y se logró determinar; como es que el internet llegó a convertirse en la herramienta importante para la comisión de estos tipos de delitos y que para ello se suma el factor humano ante los actos voluntarios de la mala fe, siendo así dos caras de una misma moneda ya que por un lado llegó a generar beneficios y a la vez se utilizó para ocasionar perjuicios, generando incertidumbre ante las exigencias de la sociedad.

Sin embargo, Mayer (2017) concluyó con una investigación que lleva por título el bien jurídico tutelado en los delitos informáticos, tuvo como objetivo revisar exhaustivamente y analíticamente las distintas investigaciones relacionadas a los delitos informáticos que protegen un bien jurídico especifico. Esto con la finalidad de entender y definir el bien jurídico. El nivel de investigación fue No Experimental estudio y comparación de tesis instrumento análisis documental con esto buscó determinar la identificación del bien jurídico específico, asociado a la función que brinda la informática, justificado por los delitos informáticos, aparte de repercutir en el soporte lógico de los sistemas y ejecución de las redes computacionales, considerando dichos puntos de gran interés en cuanto a la funcionabilidad. Por otro lado, tenemos a las redes computacionales que permite la interacción de otros sistemas brindando acciones remotas y masivas entre los usuarios constituyendo desde este punto de vista un bien jurídico de uso colectivo que debería ser considerado para su tutela.

Importante también, Cortés, Ballén y Duque (2015) concluyeron, mediante un artículo de investigación que lleva por título La persecución judicial contra los delitos informáticos en el distrito judicial de Villavicencio. Tuvo como objetivo identificar la cantidad de investigaciones asociados a delitos informáticos que fueron gestionados en la Fiscalía Seccional de Villavicencio. La finalidad fue identificar cuáles son los medios, ya sea tecnológicos, humanos entre otros con los que cuenta la policía judicial para confrontar actos respectos a delitos informáticos El nivel de investigación fue No Experimental de enfoque cualitativo y el instrumento fue entrevistas y acopio documentario. Se llegó a determinar que los medios con los que cuenta el Distrito judicial de Villavicencio son escasos lo que reflejó ineficacia ante las situaciones de denuncias por delitos informáticos 65 en el 2011 con 19 archivos y 30 en el 2012 con solamente 5 archivos.

Carrera, Quilligana, Aguilar y Fiallos (2019) concluyó mediante un artículo de investigación que lleva por título Desafío de la ciberseguridad ante la legislación penal ecuatoriana. Que tuvo como objetivo establecer punto de controversia respecto a casos de ciberdelitos, sobre la seguridad y el espacio y la intervención de la norma ante los delitos informáticos. Con la finalidad de ubicar los espacios y componentes que pudieron determinar las acciones delictivas mediante el uso de

medio informáticos, en busca de prevención a causa de la falta de conocimiento referido a las normas pertinentes. El nivel investigación fue No Experimental recolección de documentos escritos. El instrumento fue la recolección de distintos tipos de documentos dentro de ellos considerados los medios de información Nacional, como las revistas, libros, artículos científicos en relación al tema de investigación. Llegaron a determinar que se encontró los inconvenientes que suscita a la inseguridad a causa de los ciberdelitos ante la evidente situación de las normas ecuatorianas referente a este tipo de delitos debido a la falta de conocimiento de los magistrados y autoridades en cuanto al punto de vulnerabilidad de los organismos judiciales.

En cuanto a los antecedentes Nacional**,** García (2019) concluyó una investigación que lleva por título los avances de la ciberseguridad en el Perú breve aproximación al marco normativo, tuvo como objetivo analizar los distintos proyectos normativos de ciberseguridad finalidad y conocer el avance gradual de la norma frente a los ciberdelitos. El nivel investigación fue No Experimental, instrumento; análisis documental, llegando a determinar y poner en conocimiento sobre los proyectos presentados mediante el congreso del Perú ante el área de tramites, siendo estos 2 proyectos de Ley de abril del 2019, referidos a los delitos informáticos.

Por otra parte, Pardo (2018) concluyó una investigación de tesis que lleva por título Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018, tuvo como objetivo Analizar el tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018 con la finalidad comprender donde se dió el quiebre normativo, ya sea el fondo o la forma o talvez los mecanismos no adecuados. El nivel de investigación fue No Experimental, el instrumento fue recolección de datos, la guía de entrevista con 6 especialistas en el tema como entrevistados y se logró determinar que las normas jurídicas referente a los delitos informáticos contra el patrimonio es muy genérica, mostrando deficiencia ya que no es posible y lógico entender que en los fraudes informáticos contra el patrimonio podamos concebir la idea de que este considerado todas las modalidades o tipos, mostrando así posibles vacíos legales obstaculizando en la adecuada sanción efectiva de estos tipos de delitos informáticos contra el patrimonio.

Adicional a ello, Hancco (2017) concluyó una investigación que lleva por título La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017 objetivo Analizar la deficiencia regulada en la Ley 30096 respecto a la descripción del bien jurídico protegido en cuanto al tipo penal informáticos y el objeto de disminuir el alto índice del abuso sexual infantil. El tipo de investigación es mixta de diseño interpretativo el instrumento es de análisis documental y se logró determinar que la Ley 30096 referente al tipo penal informático en cuanto se considera una Ley especial y de esta no sea necesaria debido a que los bienes jurídicos en cuanto a la integridad del bien protegido es más extenso, ya que esta, es referido en el Artículo 205 de Código Penal, sancionando el daño a los distintos tipos de bienes y referente a otras normas con el fin de castigar las distintas conductas relacionado a los datos informáticos.

Sin embargo, Chávez (2018) concluyó una investigación de tesis que lleva por título El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la corte superior de justicia de lima norte 2017, tuvo como objetivo identificar como es que la intimidad personal como un derecho fundamental fue afectado a causa de los actos delictivos ante la vulneración de datos y sistemas informáticos en la Corte Superior de Justicia de Lima Norte, 2017 con la finalidad que consideró, que la intimidad personal es vulnerada ante estos actos delictivos como son acceso a los datos y sistema informáticos. El nivel de investigación fue no experimental, correlacional. El instrumento utilizado Trata de un cuestionario realizado a expertos en el tema, donde se utilizó variables. Mediante ésta se concretó que el delito contra datos y sistemas informáticos influye en un 28% en derecho fundamental a la intimidad personal.

Y, por último, Martínez (2020) concluyó mediante un artículo de investigación que lleva por título Ciberdelitos generan una batalla sin descanso a empresas y autoridades en Perú, tuvo como objetivo analizar los actos por parte de fiscalía frente a dicha situación en busca de dar garantías para prevenir la inserción en las bases de datos de los clientes. Con la finalidad de dar a conocer la problemática suscitada a causa del delito informático y las empresas afectadas en el estado peruano. El nivel de investigación fue No Experimental recopilación de datos

documentales instrumento revisión y análisis de casos, determinó que con la llegada de la tecnología también llegó los problemas ante los desafíos de prevenir ataques de los delitos cibernéticos que buscan obtener datos de clientes de los entes financieros, que están en la mira de estos individuos.

Habiendo referido los antecedentes, hemos desarrollado las categorías y subcategorías.

En cuanto al desarrollo de la categoría de los delitos informáticos. Respecto a ello Leyva (2021) concluyó:

“todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), fueron realizados con el empleo de un equipo automático de procesamiento de datos” (2021, p.34)

De lo señalado se pudo inferir que son considerados delitos informáticos siempre y cuando contra venga las normas jurídicas mediante el uso de computadoras u otras herramientas de procesamientos de datos.

Por otro lado, según Arbulú Martínez, citado en Leyva (2021) sobre los delitos informáticos señaló:

> El delito cibernético es todo comportamiento que va en contra de las leyes realizado a través de sistemas de procesamiento de datos, contra la información digital siempre en perjuicio de una persona, que podría ser natural o jurídica. Una de las características del delito informático es ser pluriofensivo toda vez que puede atentar e ir contra el patrimonio, la intimidad, la seguridad pública e informática, y esta última que puede ser considerada como una nueva modalidad de delito informático que debe ser tutelado penalmente. (p. 35)

El delito cibernético es el comportamiento que va en contra de las normas legales de una sociedad realizado mediante el uso sistemas informáticos, causando perjuicios en contra de las personas naturales o jurídicas vulnerando los patrimonios, la intimidad, seguridad pública y la seguridad informática.

Importante mencionar que Camacho (1987) citado en Aroni y Barrios (2018) sobre los delitos cibernético o informáticos consideró:

> Toda acción realizada de forma dolosa que provoca un daño a las personas o entidades y no siempre obteniendo un beneficio material para su autor, aun cuando no se ha

> perjudicado de forma directa o inmediata a la víctima, en cuya acción antijurídica intervienen de forma activa dispositivos que muy frecuentemente son utilizados y vinculados a la tecnología en las actividades informáticas (p.13).

Sin duda, son considerados delitos informáticos a todas las acciones realizadas de manera premeditada y dolosa con dispositivos generalmente vinculados a la tecnología para poder beneficiarse de manera ilícita de forma directa o indirecta.

Aunque con la expansión mundial del internet en nuestra sociedad, en los últimos años, han surgido nuevos preceptos más cercanas a nuestra realidad actual. En ese sentido Tellez (2017) citado por Aroni y Barrios (2018) señaló:

> Que los delitos informáticos o ciberdelitos son todas las acciones antijurídicas y culpables a través de vías informáticas, que tienen como objetivo destruir, manipular y dañar ordenadores, medios electrónicos y redes de Internet. Todo esto porque la informática es realmente más rápida que la legislación, aunque, existen conductas criminales mediante las vías informáticas que no son consideradas delito, según la "Teoría del delito", el cual; solo se definen como abusos informáticos, y parte de la criminalidad informática. (p.187).

Podemos decir que un delito informático es toda acción que va en contra de las normas jurídicas, con el objetivo de hacer daño mediante el uso de internet. Todo ello debido a que informática se mueve más rápido que la legislación, sin embargo, según la “Teoría del Delito”, no todos estos se consideran delito informático, solo son llamados abusos informáticos.

Teniendo en cuenta lo anteriormente mencionado es importante conocer que el uso de la tecnología en los delitos informáticos tiene la denominación de bien jurídico autónomo, fundamentalmente por las características cuantitativas y cualitativas. Por ello, el internet es usado en todo el mundo frecuentemente por millones de personas, permitiendo una comunicación en tiempo real con cualquier individuo, quedando demostrado que esta tecnología es fundamental para la sociedad mundial, por ello la importancia de su protección y tutela para todos aquellos quienes lo usan.

Por ello respecto al uso de la tecnología se dice que “la fe y la confianza en los sistemas informáticos no se ven afectados por la comisión de un delito; antes bien, su afectación se vería plasmado por la inexistencia o ausencia de sanciones tras la ejecución de comportamientos delictivos”. (Mayer, 2017, p. 09)

Los delitos informáticos contra el patrimonio tenían sentido respecto de la cibercriminalidad, porque fueron ejecutadas a través del internet mediante el uso de redes computacionales, redes sociales y otros mecanismos de la tecnología. Entonces el problema recaía en la paupérrima protección punitiva a quienes usaron la tecnología y la mala e ineficaz sanción para quienes realizaron esta comisión de delitos. Por ello su mayor afectación se produjo por la ausencia de las sanciones tras la realización de todos estos actos y comportamientos delictivos.

Asimismo, Enisa citado en Pythagoras (2021) sostiene que:

> El aumento en el uso de tecnologías de la información llevó a un aumento de las técnicas de ingeniería social, por lo que la mayoría de los ciberataques en la actualidad incluyen alguna forma de ingeniería social y estas técnicas incluyen pretextos, cebos, quid pro quo y tailgating, así como phishing y spear phishing. (P. 765).

Con el aumento del uso de la tecnología se puso en evidencia que los ciberataques han incrementado notablemente, por lo que se hacía referencia a una ingeniería social en donde se encontraron técnicas de robo de patrimonio, tales como Phising y Spear phising.

según Miró (2013) citado por la (OFAEC, 2020), detalla “delito informático como todo acto delictivo generado en el Ciberespacio con las singularidades criminológicas, victimológicas y riesgo penal proveniente de ello” (p.13).

En dicho sentido, el ciberdelito va más allá de la conducta delictiva típica que se desarrolla en el espacio físico tradicional, sino que este necesita del ciberespacio y la tecnología para desarrollarse y ser catalogado como tal.

Por otro lado, Cascavilla, et al. (2020) sostuvo que:

> El ciberdelito se llevó a cabo mediante el uso de un aparato digital o una computadora que se usó como herramienta para cometer delitos informáticos, y son los ciberdelincuentes que usaron la tecnología informática para poder acceder a información que pudo ser secreta o personal, información comercial o secretos comerciales, y además usaron la red para cualquier otro propósito malicioso. (p. 1).

Por consiguiente, los ciberdelincuentes, usaron como herramienta u objeto para delinquir, computadoras con acceso al internet, donde obtuvieron información personal, comercial u otros, todo ello con la finalidad de realizar actos maliciosos. En dicho contexto sobre el uso de la tecnología Elvis (2017) sostuvo:

> El avance de la tecnología y la aplicación en muchos ámbitos de la actividad humana muestra como resultado una clara dependencia en el uso de la tecnología, al mismo tiempo se utilice esa oportunidad para el mal aprovechamiento de personas que actúan en contra de las leyes y buscan un fin ilícito de estas oportunidades, todo aquello puede verse en los robos de cuentas vía internet y mediante la clonación de tarjetas. (p. 23).

El uso de la tecnología informática tuvo muchas utilidades, y muchos de estos medios de comunicación, tales como el messenger, correo electrónico, facebook, twitter, whatsApp, instagram entre otros, sirvieron para manipular el procesamiento de información digital. Por lo tanto, todos estos avances de la informática y su aplicación a casi todos los quehaceres de la actividad humana trajeron como resultado el perjuicio patrimonial de las personas naturales y jurídicas, todo ello se vió reflejado en la sustracción de dinero de muchas cuentas bancarias.

Sin embargo, para Okutan (2019) quien sostuvo:

> Hay muchas formas de detectar un delito cuando se encuentra con un delito cibernético y así mismo, hay formas de proteger esos delitos antes de que sean procesados, por consiguiente, los piratas informáticos quienes siempre están listos para infiltrarse en las redes, no tendrán acceso fácil, por ello; los IDS, Firewall y Honeypot son tecnologías importantes que evitaron que un atacante ingrese a la red.

Existieron alternativas muy importantes para proteger nuestra privacidad cibernética, el cual nos permitieron evitar que delincuentes ingresen a nuestras redes y roben nuestros patrimonios, estas tecnologías que pudimos usar son los IDS, Firewall y Honeypot; sin duda alguna, evitaron el acceso fácil cuando se quiso delinquir.

Respecto al uso de la tecnología en los delitos informáticos Patil y Devane (2019) sostuvo que: “Un aumento de la digitalización dio lugar a delitos informáticos, en donde los protocolos de red existentes fueron insuficientes para recopilar la

evidencia digital requerida del delito cibernético, lo que eventualmente dificultó el proceso de investigación forense".

Sin lugar a duda, el uso excesivo del internet ha producido aumento de los delitos informáticos, y lo que se evidenció con estos incrementos, fue la dificultad para obtener evidencia digital al realizar el proceso de investigación forense de los ciberdelitos.

Ministerio Público Fiscalía de la Nación, Oficina de Análisis Estratégico contra la Criminalidad (OFAEC, 2020); la OFAEC (2020) señala:

> El año 2014, el Perú requirió ser parte del convenio de Budapest, el Consejo Europeo aprobó lo requerido el 2015. Para el 12 de febrero de 2019, el Congreso aprueba dicho Convenio, mediante Resolución Legislativa N° 30913 validado, por el Ejecutivo, mediante D. S. N° 010-2019-RE, del 09 del 03 del 2019, generándose el día 01 del 12 de 2019 como fecha de inicio en vigor. Así actualizando nuestra legislación a los artículos del convenio de Budapest, dentro de ello el capítulo v delitos informáticos contra el patrimonio artículos 8 de la Ley N° 30096, y modificatoria ley 30171. (p. 14).

Podemos conocer que el Estado de Perú, desde marzo 2014 adecuo la Ley N° 30096 de delitos informáticos mediante la Ley N° 30171 conexo a los artículos del convenio de Budapest

Otro aporte de la ORACE (Oficina de racionalización y estadística) enviado a la OFAEC (Oficina de Análisis Estratégico contra la Criminalidad) del Ministerio Público y Fiscalía de la Nación; donde efectivamente dan a conocer que al año 2020, los delitos informáticos contra el patrimonio cubren el 42% del total general de delitos informáticos.

Al respecto, el derecho colombiano en su_STP6279-2017, 4 de mayo de 2017, sostiene que:

> Se denominó autor de delitos informáticos aquellos que accionaron con hechos punibles de robo mediante los medios informáticos, con el empleo de la tecnología para vulnerar datos privados, cometiendo actos criminógenos y teniendo acceso abusivo a sistemas informáticos, realizando actos gravosos de violación de datos, falsedad en documento privado y conciertos digitales para delinquir.

Los delincuentes cibernéticos actuaron con el empleo de medios informáticos, incurriendo en el concurso heterogéneo de delitos agravados tales como: violación de datos, falsedad en documento privado y conciertos para delinquir.

Habiendo conocido lo mucho que influyó la tecnología para la comisión de este tipo de delitos informáticos dando como resultado la vulneración de derechos de las víctimas; individuo, sociedad y Estados, ocasionando daños y perjuicios de distintas índoles, para tener una idea, se mencionó una situación real en el país de México año 2017, y en cuanto a los perjuicios (Octavio Islas) señaló:

> Que en el estado de México varios medios de comunicación informaron, que muchas instituciones financieras sufrieron ataques cibernéticos y así lo reconoció el señor Alejandro Díaz de León Carrillo, Gobernador del Banco de México, y el señor Marcos Martínez G. presidente de la Asoc. de Bancos de México. (2018, p. 01)

Con dicha información de gran relevancia que nos dio a conocer que el 17 de abril 2017, el primer victimado fue la casa de bolsa; después de ésta, el segundo ataque se dio el 26 de abril 2017 y afectó a Banorte, y otros centros financieros e instituciones que reconocieron quiebre en su seguridad de prevención.

Tengamos en cuenta que, en la mayoría de situaciones o casos, la comisión de un delito cibernético se detectó de manera fortuita. Y cuando esta acción afectó a una persona jurídica o natural, muchas veces no se realizó la correspondiente denuncia debido a la mala reputación o publicidad que se pudo generar en el mercado.

Respecto a estos daños se mencionó que “La delincuencia cibernética generó grandes daños y perjuicios a la víctima, principalmente en el carácter económico, pero el mayor daño es causar una mayor alarma en la sociedad”. (Leyva, C. 2021, p.40)

En lo que respecta a los daños o perjuicios ocasionados por estos actos delictivos, fueron de tal magnitud que muchas veces fue preferible no denunciar porque la

sanción económica al infractor fue menor al daño causado ante la sociedad. Rachana & Devane (2020) sostuvo:

> Debido al desarrollo cada vez mayor de la digitalización, las amenazas a la seguridad cibernética han aumentado y asegurar la red se ha convertido en el trabajo de misión crítica de un administrador, todo ello se vio plasmado en las estadísticas actuales sobre el delito cibernético en la India donde muestrearon que el número de casos registrados de delito cibernético fue mucho mayor que la cantidad de detenciones.

Con los cambios que sufrieron las sociedades en el mundo, la ciberdelincuencia ha aumentado de manera desmedida, a tal punto de llegar a cifras muy críticas, en donde incluso los administradores de justicia no pudieron detener a todos estos delincuentes. Por lo tanto; las personas han tenido grandes perjuicios a causa de estos atentados cibernéticos y evidencia una realidad que no se pudo hacer mucho para detenerlos.

Por otro lado, respecto a los Daños o perjuicios Ashikin et al. (2017) sostuvieron que: “Los comportamientos maliciosos de los usuarios debido a la falta de conciencia, como la descarga de aplicaciones no autorizadas y el acceso a datos confidenciales utilizando una red insegura, permitieron que se produzcan más ataques”.

Son los mismos usuarios quienes usaron de manera desmedida e irresponsable las redes, en donde muchos de estos realizaron descargas prohibidas, exponiendo sus patrimonios, los cuales fueron aprovechados por los ciberdelincuentes para poder delinquir y obtener datos confidenciales, posterior a ello accionando maliciosamente y causando enormes perjuicios contra los patrimonios.

Habiendo ya resaltado puntos importantes como los medios que influyeron, los perjuicios y el mismo contexto del delito informáticos, pues se disertó sobre los perjuicios en cuanto al patrimonio.

Partiendo de la definición de patrimonio Mayer sostuvo:

“El patrimonio o bien es una universalidad jurídica, que está compuesta por activos y pasivos, y éstas pudieron resultar afectados por uno o más comportamientos delictivos afectando dicha universalidad” (Mayer Lux, 2017, p. 47).

Por tanto, se pudo inferir que el patrimonio es lo que se posee siendo el conjunto de éstas, referido al activo como los bienes y los derechos que son tangibles o intangibles; y el pasivo aquellas que originaran la diferencia dando como resultado el patrimonio, donde en situaciones de actos delictivos afectaron directamente a los activos.

Asimismo, Vásquez, Regalado y Guadron acotaron que el fraude informático es el "perjuicio patrimonial generado a otra persona mediante la manipulación de datos informáticos o la interferencia en el funcionamiento de un sistema informático, cuya finalidad es la obtención ilegítima de un beneficio económico para sí o terceras personas" (2017, p. 65).

Evidentemente como mencionó el autor en cuanto al patrimonio; esta se ve perjudicado en aspectos económicos ante la comisión de estos delitos informáticos, ya que como se mencionó en la anterior cita podríamos relacionar a este perjuicio o pérdida económica como una forma de pasivo que ocasionara una diferencia en el resultado total del patrimonio de la víctima.

Sobre las modalidades de delitos informáticos contra el patrimonio Pardo (2018) mencionó "que específicamente dentro de cada tipo de delitos se podría identificar otros sub categorías de delitos, por lo tanto, dentro de delitos cibernéticos o informáticos contra el patrimonio podemos identificar al hurto, fraude, estafa y los sabotajes informáticos" (p.39)

De esto entendimos que, tomando como caso en los delitos informáticos contra el patrimonio, estos conllevaron a relacionar el acto a otros modos de delitos para poder delinquir ya sea utilizando, manipulando o incluso modificando la información sustraída y con estas afectaciones; vistas como estafa maestra, las cuales darán respaldo en sí a producirse otros modos de delitos informáticos contra el patrimonio.

Por otro lado considerando que la afectación al bien, mediante estos tipos de delitos informáticos contra el patrimonio conllevaron muchas veces a un perjuicio del bien en valor económico, mencionado en el artículo de ius 360; sobre las modalidades de delitos, Zevallos (2020), mencionó " respecto al bien jurídico, se

protege principalmente la información, considerada de diferentes formas, ya sea como un valor intrínseco a la persona, como un valor económico *(…)*; en otras palabras, se tienen que proteger el bien jurídico tradicional (2020, p. 1).

Con ello entendimos que no tan solo se afecta a la información, si no a causa de este acceso a la información quedamos vulnerables a que se afecten otros tipos de bienes jurídicos tradicionales, entendido no solo como bien inmaterial sino también material, por ejemplo, al usar la información de claves cuentas encriptadas y de cifradas para sustraer dinero, e incluso para alterar comprar virtuales y modificar la dirección de entrega.

Respecto a las nuevas formas de delitos informáticos Ruiz (2018) señalo:

> La innovación tecnológica ha causado el origen de nuevos fraudes donde por medio se manipula la informática, mediante artificios semejantes que están lejos de la concepción real. Dentro de ellos tenemos el Pharming está da ventaja sobre la debilidades o vulnerabilidades en el sistema software de los servidores DNS o en los equipos de los usuarios de Internet para redirigir electrónicamente, a través del uso de ingeniería informática, una razón o nombre de dominio a diferente sitio, controlado por el delincuente que suele imitar las páginas legítimas, como por ejemplo, de las entidades bancarias, con el fin de captar datos personales del propietario y usarlos con delictuosamente. Así mismo, el del virus troyano, conocido mundialmente como Ransomware, aplicados siguiendo parámetros prefijados de navegación web, se activa permitiendo el bloqueo del equipo informático y encriptando todos sus contenidos. De esta manera, lo que se busca es inducir a la víctima y hacer abonar ciertas cantidades de dinero, ya sea mediante engaños o hacerlo coactivamente, obteniendo la información perdida. (p. 09)

Pues con esto el autor no dio a conocer que los nuevas modalidades o formas de delinquir respecto a los delitos informáticos, salieron del concepto común descrito y entendido por las normas, llevando así a la necesidad de entender que nuestra legislación necesita cambios más acordes a esta realidad que día a día avanza.

En cuanto a los efectos como causa de dichos delitos Lux (2018) detalló:

> consecuencias inmediatas y medianamente mediatas de la cibercriminalidad. Al respecto, los delitos de espionaje, sabotaje y fraude informático; casi siempre repercuten o tienen incidencia en diversos intereses de titularidad de las víctimas, que en lo posterior se verán afectados, de acuerdo al comportamiento delictivo que se haya cometido. Cuando se trate de víctimas que son personas naturales, sus patrimonios o

> intereses se identificarán, con su intimidad o privacidad, o con sus bienes. Cuando las víctimas son personas jurídicas o empresas, dichos delitos perjudicarán principalmente sus intereses patrimoniales. (p. 193).

Teniendo en cuanto a lo mencionado la afectación no solo compete a los intereses patrimoniales si no adicional a ello a aquel margen relacionado a la intimidad o privacidad asociado al patrimonio del cual podría obtenerse algún beneficio en cuanto al conocimiento de esta.

Al respecto la Sentencia del Tribunal Constitucional N° 1100/2020, 10 de diciembre del 2020, sostiene:

> El actor logró manipular el sistema informático del password que se le entregó para el desarrollo de sus labores y la de otros trabajadores, con lo cual logró efectuar retiros de las cuentas de plazo fijo de los clientes de la financiera, para disminuir el saldo de capital de las mismas y apropiarse de dichos montos.

Los delincuentes informáticos aprovechando sus labores, efectúan maniobras con el empleo de computadoras y el internet para delinquir y realizar robos sistemáticos, afectando el patrimonio de las personas.

Asimismo, podemos tener idea de otros modos que se desprenden y son afectados por los delitos informáticos, al respecto (Ruiz) señalo:

> De hecho, esta disposición legal también ha frenado la denuncia de las ciberestafas, que, a pesar de ello, siguen siendo el delito informático por el que se inician más procedimientos judiciales. Un 61,5 % de las estafas que se realizan a través de Internet llegaron a los tribunales o al Ministerio Fiscal en 2018, muy por debajo del dato de años anteriores a la citada reforma, en los que se superaba el 80 %. De ello se deduce que las investigaciones por estafas en la red son las que con mayor frecuencia y en mayor número se denuncian sin ser trasladadas a los tribunales porque no se identifica al autor. (2018, p. 09).

Claramente vimos que los afectados, en este caso llamados las víctimas, denunciaron este tipo de delitos cibernéticos, pero nuevamente el gran inconveniente, de que mucho de estas denuncias no se llegaron a formalizar por la falta de identificación del autor, ocasionando en la víctima una situación de

vulnerabilidad con consecuencias y repercusiones en su integridad emocional, psicológica y moral entre otros,

La INTERPOL (2017). Mencionó que.

> La ciberdelincuencia es un fenómeno sin fronteras, y ante ello, los organismos encargados de su regulación mediante la aplicación de sus leyes tienen problemas para hacerlo eficazmente; puesto que sus investigaciones tienen límites transfronterizos haciéndolos ineficaces frente a los problemas de tipo jurídico y la diversidad de sus capacidades en el mundo.

De ello la clasificación de los delitos informáticos fueron muchos, dentro de ellos encontramos: Contra sistemas y datos informáticos, equipos de redes infectados manipulados remotamente), Estafas mediante Internet, virus, Phishing (obtención de información personal confidencial mediante fraude, Distribución de imágenes índole sexuales contra menores y Usurpación de la identidad.

Para nuestra legislación peruana, en la Ley 30171, los tipos de delitos enfocados a los bienes jurídicos protegidos se pueden clasificar en: delitos informáticos contra el patrimonio, delitos contra la persona, delitos contra la fe pública, delitos contra la seguridad, delitos contra los datos informáticos y los sistemas informáticos.

Pues pudimos identificar un tipo de delito asociado a otro, con ello generando diversidad en cuanto a los tipos de delitos informáticos mostrando así una falta de uniformidad y desenlace estrechamente asociado a la clasificación de estos tipos de delitos

Con respecto al Marco Jurídico Internacional de los delitos informáticos se establecieron distintos medios con el fin de hacer frente, dentro de ello acuerdos, convenios, conferencias y distintos parámetros enfocados en busca de posibles soluciones, uno de los convenios más importantes es el de Budapest. Esta organización creada el año 2001 (Hungría) inicialmente conformada por distintos países europeos con el fin de tratar actos delictivos asociados a Cibercriminalidad en busca de medios provisorios y una adecuada legislación acorde a dicha realidad que es limitada por aquel llamado ciberespacio.

Cabe mencionar que el Perú se unió al mencionado convenio el 2019.

Por otro lado, nuestro Perú no es ajeno a esta realidad, sin lugar a dudas, se vio afectado por los delitos informáticos asociados a los avances tecnológicos, por ello (Cconislla) mencionó sobre tecnología “punto que permitió el desarrollo de la sociedad y a la vez esta generó nuevas opciones ante las conductas delictivas en el marco legal” (2017, p. 52).

Con lo mencionado ´por el autor ante las circunstancias de los nuevos avances tecnológicos entendimos como algo positivo para la sociedad, también permitió el acceso a situaciones negativas para la oportunidad de cometer ilícitos informáticos.

.

Ya conocido sobre las distintas etapas normativas, que fueron asociados a los delitos informáticos en el Perú, se conoció que la primera norma se dio mediante el Código Penal de 1991, Articulo 186 , es cual señaló como un agravante del delito de hurto, Después de esta se emitió la Norma de delitos informáticos en el C.P. mediante el capítulo 10, descrito en el artículo 207A hasta el 207D debido por distintas situaciones buscando que las normas se acoplen a la realidad y exigencia, se decidió por categorizar como norma especial a los delitos informáticos, a causa de esto se derogaron todas las normas anteriores y emitió la Ley 30096, posteriormente con el ingreso de Perú al Convenio de BUDAPEST se modificó la ley antes mencionada mediante la Ley 30171.

Esta se dio con el fin de modificar los estándares legales que se vivía en el Perú, por ello se modificó la redacción típica de los artículos 2, 3, 4, 7, 8 y 10 de la referida ley. Por ello conociendo la evolucion en cuanto a estos tipos de delitos, se ubtuvo una referencia en las siguientes figuras, donde se pudo observar los márgenes de avances porcentuales en cuanto a períodos anuales del 2018 y 2019 referido a los delitos informaticos y delitos informaticos contra el patrimonio.

Cuadro N° 1

Delitos registrados en fiscalías provinciales penales y mixtas según tipo de delito sub genérico a nivel nacional – Ley N° 30171, Ley de los delitos informáticos 2018 ,2019 y 2020.

DELITOS SUB GENÉRICOS	2018	2019	2020	
	N° DELITOS	N° DELITOS	N° DELITOS	%
	LEY N° 30171 LEY DE DELITOS INFORMÁTICOS			

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO	1657	3228	1138	42%
DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA	160	335	116	4%
DELITOS CONTRA DATOS Y SISTEMA INFORMÁTICOS	159	281	79	3%
DELITOS INFORMÁTICOS CONTRA LA IMDEMNIDAD Y LIBERTAD SEXUAL	137	115	25	2%
DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	72	68	40	1%
DISPOCISIONES COMUNES	32	62	15	0.7%
SIN ESPECIFICAR DELITOS SUB GENÉRICOS	2431	4415	1325	48%
TOTAL	**4648**	**8504**	**2738**	**100.00**

Sistema de información de apoyo al Trabajo Fiscal – SIATF y Sistema de gestión Fiscal SGF.

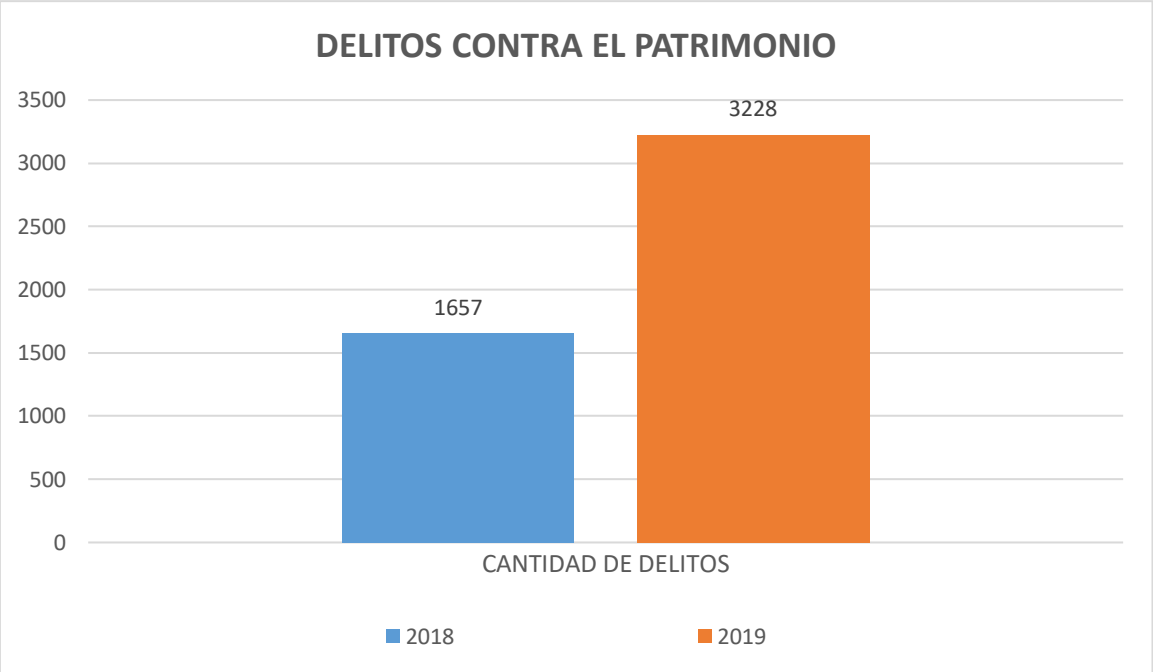
Elaborado por Oficina de racionalización y estadística ORACE.

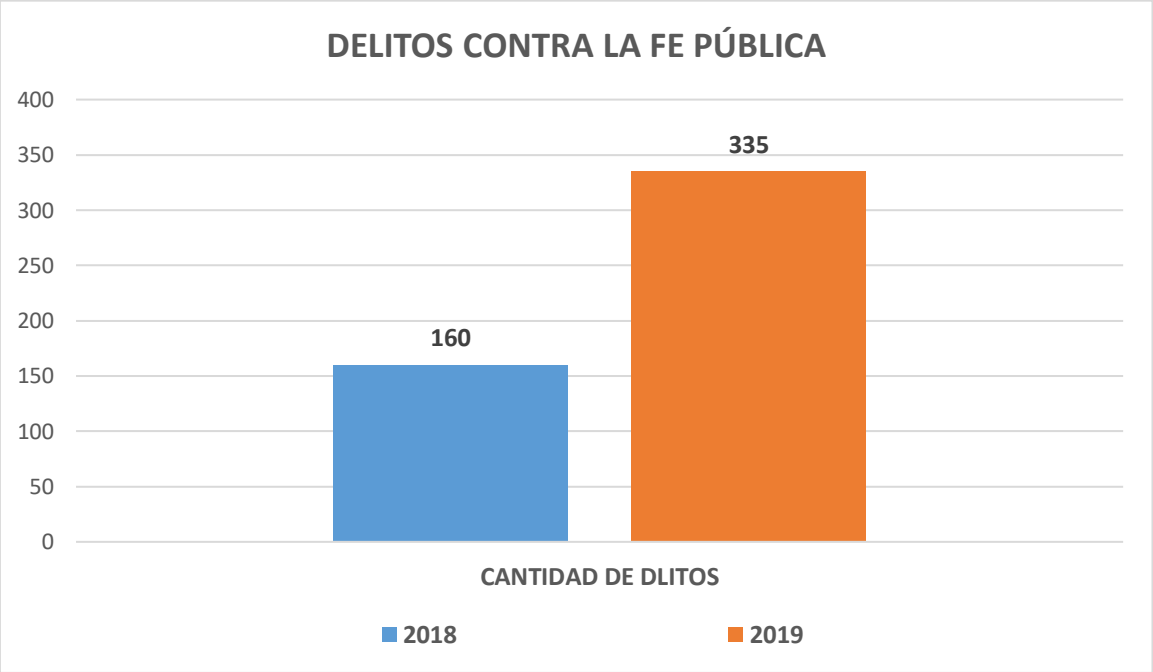
Fuente de información: Boletín estadísticos del Ministerio Público (2020).

Figura 1: Datos de Delitos registrados en fiscalías provinciales Penales y Mixtas según tipo de delito sub genérico a nivel Nacional – Ley N.º 30096, sobre los Delitos Informáticos 2018 y 2019

Aquí encontramos, del periodo 2018, del total de delitos informáticos ingresados a nivel nacional, reflejados en un total de 1657 casos, fueron delitos informáticos contra el patrimonio. Dicha cifra aumentó considerablemente para el periodo 2019, llegando a un margen de 3228 casos de delitos informáticos contra el patrimonio equivalente a (42%) del total de los delitos informáticos registrados a nivel nacional.

Cuadro N° 2
DELITOS DE MAYOR INCIDENCIA, 2018 Y 2019





Fuente de información: Boletín estadístico del Ministerio Público (2020).

Figura 2: Delitos de mayor incidencia 2018 y 2019

Otra observación fue el índice elevado que compete los delitos informáticos contra el patrimonio, ya que estos son los que alcanzan los márgenes porcentuales más altos a comparación de los otros tipos de delitos informáticos, en el periodo 2018 en relación al 2019.

Por otra parte, recurriendo al Derecho comparado sobre legislaciones de los Delitos informáticos de otros países como, Brasil, pues dicha legislación no cuenta con una Ley especial fuera del código penal.

La Ley 12737 del 2012 es una Ley que insertó modificaciones, actualizando los tipos penales asociados a los delitos informáticos, como los: artículos:

- Artículo 154-A, señala “Hackear el dispositivo de la computadora de otra persona”,
- Artículo 154-B “acción criminal en los delitos tipificados en el artículo 154-A,
- Artículo 266, refiere “perturbar los servicios telemáticos o de información".
- Artículo 298 señala sobre “falsificación de tarjeta”

También cuenta con agravantes, si media la divulgación, comercialización o transmisión a terceros de datos y cuando la víctima es un sujeto calificado.

En cuanto a la pena**,** Invadir, violentar un dispositivo informático ajeno, con el fin de obtener, manipular o destruir datos o información, pena de 3 meses a 1 año, La pena aumenta 1 sexto a un tercio si esta resulta en daño económico.
Invasión de información confidencial, comercial industrial, pena 6 meses a 2 años

A si mismo tenemos a la legislación del país de Bolivia con la Ley 1768 de (1997), dicha Ley no es un cuerpo normativo separado del código penal, sino es una ley que modifica y añade figuras típicas buscando actualizar los delitos informáticos.

En su capítulo XI, del título XII delitos contra la propiedad, del libro segundo, en él se adiciona 2 artículos:

Artículo 363 bis y 363 ter, las cuales refieren a la manipulación informática, alteración, acceso y uso indebido de datos informáticos, las penas son:

- Artículo 363 bis; pena de 1 a 5 años.
- Artículo 363 ter; pena de 1 año.

Por otro lado, tenemos al país de Argentina, dicha legislación no cuenta con una Ley independiente, que regula este tipo de delitos en un cuerpo normativo separado del Código Penal.

Ley N° 26388 del (2008), dicha ley modifica y regula los delitos informáticos en el código penal argentino, tenemos delitos informáticos contra la integridad sexual, contra la libertad, contra la propiedad, entre otros.

Sobre los delitos informáticos contra la propiedad, en este se estructura la Estafa, defraudación y Daño informático.

La estafas y defraudación se encuentran en el libro segundo, título 6, capítulo 4 en su Artículo 173, incisos: 15 modificado por la Ley N° 25930 (2004), refiere a la defraudación con uso de tarjetas débito o crédito, obtenida resultado de falsificar, adulterar, hurto, robo, perdida, ardid, engaño, o uso no autorizado de sus datos, con pena de 1 mes a 6 años de prisión.

Inciso 16, refiere al que defraude mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos, con pena de 1 mes a 6 años de prisión.

Capítulo 7, Daños referido al sistema informático, mediante los siguientes:

- Artículo 183, pena de 15 días a 1 año al que alterare, destruyere, inutilizare o vendiere, datos, documentos, programas o sistemas informáticos, si el hecho no conforme otro delito más penado.
- Artículo 184, inciso 5 y 6 refiere a daños sistema informáticos de servicio público, pena es de 3 meses a 4 años prisión (entendido como agravante)

En cuanto al país de Chile, dicha legislación si cuenta Leyes especial e independiente.

La Ley 19223 “Relativa a Delitos Informáticos” de acuerdo a su propio título, donde regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos.

Ley 20009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos.

Ley 18168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación.

El 22 de marzo, mediante Boletín aprobado 12 192-95, se deroga la ley N° 19223 reestructurando los cuerpos legales a fin de adecuarlos al convenio de Budapest. Constando la regulación de 21 artículos, tipificando conductas como: ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita, ataque a la integridad de los datos informáticos, falsificación informática, receptación de datos, fraude informático y el abuso de dispositivos. Asimismo, incorpora una nueva figura a la receptación de datos, procedimientos y permitirá promover la colaboración pública-privada a fin de mejorar la investigación penal.

En cuanto a mejoras se adicionó, ilícitos actuales como la falsificación y fraude informático, también la receptación informática, y el secuestro de datos informáticos como él (Ransomware)

III. METODOLOGÍA

El presente trabajo de investigación, es de enfoque cualitativo; por la razón que nos permitió poder analizar distintos aspectos en busca de un amplio entendimiento a ciertos contextos y situaciones de la realidad, y así permitió estructurar un conocimiento más visible a la conciencia, de tal forma que lo acontecido en base a la realidad subjetiva fue el punto de estudio. Rodríguez señaló que “Los elementos cualitativos refieren a descubrimiento, exploración, generación de teorías, etc.” (2019, p. 04).

Con ello entendimos por el autor, que el enfoque cualitativo trata de escudriñar sobre bases teóricas; para así comprende y hallar nuevos conocimientos.

En ese sentido (Díaz Herrera), señaló que “De esta forma, se describe los estudios cualitativos, que no refieren específicamente a una medición numérica, más bien demostrar expresiones culturales y sociales a través de la interpretación entre observador y observado”. (2018, p. 124)

Claramente una vez más tuvimos la noción de que el enfoque cualitativo para el autor aconteció sobre situaciones sociales que motivó el estudio, con el fin que mediante la observado se pueda comprender ciertas situaciones.

Por otro lado, el trabajo de investigación es de tipo básico; porque buscamos explicar, aclarar y entender las cuestiones planteadas en la investigación, esta que a su vez es de diseño interpretativo basado en el estudio de casos; en cuanto a las distintas situaciones a llegadas aun mismo tema de estudio, dado que se tuvo como objetivo examinar detalladamente los fenómenos asociados a las categorías de estudio, para ello utilizamos como medio de desarrollo un determinado campo del marco legal; que es el ámbito penal, relacionados a los Delitos informáticos contra el patrimonio, en cuanto a la subcategorías consideramos la intervención del uso de tecnología, los perjuicios y modos relacionados a los delitos informáticos: de todo ello separamos y consideramos aspectos importantes de esta, que nos permitió conocer sus características entre otros. Para definir el diseño de la investigación Nizama, M. y Nizama, L. sostuvo:

> Implica una finalidad instructiva ya que origina una visión analítica e ilustrativa, en cuanto a la relación o nexum entre el enfoque cualitativo y la investigación jurídica. Asimismo, es útil saber por nosotros mismos que el enfoque cualitativo sí es realmente un aplicativo en la tarea que tiene el jurista de resolver los problemas de la realidad socio jurídica. (2020, p. 70).

El escenario de estudio lo enfocamos en el mismo Marco Legal Peruano, asociado al contenido sustantivo de la norma penal, señalado en la Ley N.º 30171 sobre delitos informáticos específicamente referido al artículo 8 de la Ley, de tal modo basándonos en la información que obtuvimos de las distintas fuentes relacionados al tema.

Por otro lado, sobre en el presente estudio como participe orientado al aporte sustancial de nuestro proyecto de investigación incluimos distintos análisis documentarios jurisdiccionales; como pueden ser los expedientes, jurisprudencias, doctrinas, casaciones, revistas jurídicas indexadas, tesis, derecho

comparado, entrevista a participantes especialistas asociados al escenario de estudio, entre otras fuentes de información asociados al tema.

Díaz Herrera refirió “En términos metodológicos, como la unidad de análisis que se objetualiza como documento”. (2018, p. 132).

PARTICIPANTES ENTREVISTADOS (ESPECIALISTAS EN EL TEMA)			
01	Juez Superior	Montesinos Córdova, Clenin	Corte superior de Justica Huánuco
02	Juez Superior	Tohalino Alemán, Víctor	Corte Suprema de Justicia Lima Este
03	Juez Penal Superior	Vizcarra Pacheco, Edgar	Corte Suprema de Justicia Lima Este
04	Juez Penal Superior	Huaytalla Pillaca, Guisella	Corte superior de Justica del Callao
05	Fiscal Adjunto Pro.	Guerra Soto, Cristhian Miguel	1ra. Fiscalía Provincial Penal Corporativa de S.J.L.
06	Notario	Zambrano Rodríguez, Lucio Alfredo	Notaria Zambrano y Docencia Uni. S.M.P.
07	Abogado	Cerón Salazar, Nelson	Docencia Universidad Inca Garcilaso de la Vega
08	Abogado	Hinostroza Rodríguez, Carlos	Abogados J.P.
09	Abogado	Balcázar Chilcho, Jaime	Grupo Themis Abogados SAC
10	Abogado	Coaguila Tapia, Percy	Grupo Themis Abogados SAC

Asimismo, utilizamos como técnica; la entrevista y como instrumento de recolección de datos; la ficha de entrevista, para ello hemos contando con el apoyo de especialistas quienes brindaron su aporte en cuanto a preguntas respecto al tema, el cual generó un mayor acotamiento a nuestro proyecto de investigación, (Lizandra y Peiró) mencionaron que “ la credulidad del estudio se basa en la

demostración de las transcripciones de las entrevistas y los actos de contraste y crítica realizada por el equipo de investigación" (2020, p. 43)

Claramente entendimos, cuán importante es contar con el aporte de especialistas en el tema, de esta manera nos permitió poder disertar sobre aquellos posibles vacíos legales o deficiencias asociadas al tema de investigación.

En cuanto al procedimiento a fin de recolectar la información mediante los instrumentos, lo que hicimos es proceder a efectuar interrogantes mediante la ficha de entrevista, interrogantes asociadas a los problemas específicos y generales en cuanto a las categorías y subcategorías relacionados al tema de investigación, para que los entrevistados; en este caso especialista jurídicos en el tema, que nos brindaron su aporte basado a su experiencia del día a día.

Referente al método utilizados, fueron el analítico y hermenéutico, el primero basado en el análisis de datos, pues analizamos los distintos aportes de los especialistas jurídicos. en cuanto a las interrogantes generadas mediante el instrumento; en este caso la ficha de entrevista la cual consta de 9 preguntas en total y los aportes del marco teórico. En cuanto segundo método nos permitió analizar la norma del artículo 8 de la Ley 30171.

El presente trabajo de investigación cumple con los parámetros de rigor científico pretendido, en cuanto a la credibilidad y fiabilidad ya que se obtuvo los datos de fuente confiables citadas según Norma APA, por otro lado adquirimos la fuente de información que ha proporcionado certeza y confiabilidad, también se han utilizado las técnicas e instrumentos de recolección de datos como es el caso de la ficha de entrevista y análisis de datos, en cuanto a todo ellos de acuerdo al tipo, enfoque, diseño y nivel de la investigación.

VALIDADOR	% DE VALIDACIÓN
Dr. Prieto Chávez, Rosas Job	94%
Dr. Montesinos Córdova, Clenin	95%
Mg. Balcázar Chilcho, Jaime	95%

IV. RESULTADOS Y DISCUSIÓN

Obtuvimos los resultados de las interrogantes de entrevista, estos se formularon acorde a los objetivos planteados, en concordancia a las categorías y subcategorías.

Respecto a la primera interrogante asociado al objetivo general, buscando conocer la experiencia de los entrevistados, sobre la intervención del Estado y como es que este, debería afrontar los delitos informáticos. La mayoría de los entrevistados, principalmente Huaytalla , Vizcarra y Montesinos (2022), señalan que debido a la pandemia por la COVID 19 y avances tecnológicos, es necesario que el Estado, para enfrentar a la llamada criminalidad informática, los tipos penales tradicionales sean revisados, sean actualizados para así consolidar la seguridad jurídica a través de una regulación eficaz de nuestra normativa penal, ello a través de un nuevo estudio y análisis correspondiente a través de los organismos, accionando una serie de controles necesarios para su afrontamiento.

Teniendo en cuenta la intervención del entrevistado Guerra Soto (2022), menciona que el Estado debería actuar en cuanto a capacitación y conocimiento actualizado, tanto para magistrados, fiscales, peritos, abogados y personal policial, entre otros. Segundo trabajar sobre la falta de coordinación y comunicación, no tan solo entre personal asociados al derecho sino la interacción con especialistas ya sean técnicos, ingenieros, especialistas en software.

Por otro lado, resaltando el aporte del entrevistado, Cerón (2022), señala que el Estado peruano debería promover los convenios multilaterales que ayuden a disminuir los delitos informáticos, con ello tener la cooperación mutua con otros Estados para la persecución de estos delitos.

En cuanto al resultado de la segunda interrogante asociado al objetivo general**,** sobre si se considera que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio. Todos los entrevistados, señalan que si influye, puesto a que el avance de la tecnología informática aún más dada la coyuntura de la COVID 19 y su influencia en casi todas las áreas de la vida social, sobre todo para la interacción en nuestras actividades; como comunicarse, informarse, realizar movimientos económicos, entre otros, pues el uso de la tecnología se ha

convertido en uno de los principales factores que ayudaron al incremento de los delitos informáticos contra el patrimonio, principalmente porque los agentes activos, valiéndose de sus conocimientos de la informática que les permite traspasar las barreras del espacio, tiempo y así burlar la seguridad, perjudicando a las víctimas mediante la comisión de estos delitos beneficiándose ilícitamente de sus bienes patrimoniales.

Resaltando el aporte del entrevistado Vizcarra. (2022), quien menciona que la falta de educación sobre las amenazas informáticas, concientización, la poca alfabetización digital y tendencia innata del ser humano a confiar, permitió que los atacantes se aprovechen y vulneren sus patrimonios.

Otro importante aporte de la entrevistada Huaytalla (2022), señala que la tecnología es un agregado de conocimientos técnicos, que permite crear, modificar, y así adaptar nuestro entorno, facilitando las actividades del hombre, siendo prescindible la presencia física, convirtiéndose así en el medio del cual se vale el sujeto activo, para no ser descubiertos y así cometer este tipo de delitos informáticos contra el patrimonio.

Respecto a la tercera interrogante asociados al objetivo general sobre si los entrevistados Consideran que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021. La mayoría de los entrevistados resuelven que las leyes no son acordes a nuestra realidad, en tanto que los cambios tecnológicos en la informática son constantes después del factor COVID-19, en la que, en todo ámbito particular y público se valen de la informática, para el desarrollo de las actividades y sobre la cual en forma constante se producen comportamientos ilícitos por parte de los agentes activos, comportamientos que no se encuentran reguladas en la ley 30171 que fue publicada en el diario oficial el peruano, 10 de marzo del 2014, es necesario una mejor y clara tipificación de los delitos informáticos contra el patrimonio, toda vez que a raíz de la pandemia se han incrementado este tipo de delitos.

Resaltando el aporte del entrevistado Vizcarra y Tohalino (2022), quienes menciona que el desarrollo y masificación de las nuevas tecnologías de la información en tiempos de pandemia, han dado lugar a cuestiones, tales como; el

análisis de la suficiencia del sistema jurídico actual para regular las nuevas posiciones, los nuevos escenarios, en donde se debate los problemas del uso y abuso de la actividad informática y su repercusión en nuestra realidad actual.

Por su parte el Entrevistado Vizcarra. (2022), detalla que, según el reporte de ciberseguridad 2020 del BID y OEA- Riesgos, Avances y el Camino a seguir en América Latina y el Caribe, el Perú aun no cuenta con una estrategia nacional de seguridad cibernética.

A si mismo el entrevistado Guerra S. (2022), indica que la norma falta especificar respecto a las formas o modos. Entre ellos los relacionados con los fraudes que afectan a la manipulación electrónica de las tarjetas débito o crédito, que son unos de los más frecuentes.

Por otro lado y en sentido opuesto a los demás entrevistados, Cerón (2022), señala que nuestras leyes si están reguladas acorde a nuestra realidad, el problema radica en la interpretación de estas leyes por parte de algunos colegas, quienes por la falta de capacitaciones en la cuestión informática, no aplican de manera adecuada la Ley 30171, la citada norma incorporó una serie de delitos informáticos, dentro de los que se encuentran interceptación de información, suplantación de identidad, entre otros, a estos tipos penales se les establecieron sanciones penales con la finalidad de contrarrestar su consumación, pero ya depende de los operadores de justicia aplicar las leyes correctamente.

Acotación adicional, de Huaytalla (2022) quien mantiene una postura intermedia, mencionando; que no tan solo debería revisarse la norma a consecuencia de la pandemia, sino que principalmente debería revisarse si hay un adecuado procedimiento por parte de los operadores de justicia, en cuanto a si estos están correctamente capacitados, si cuentan con los implementos logísticos, entre otras cosas.

En cuanto al resultado de la primera interrogante asociado al objetivo específico 1, sobre el artículo 8º de la ley n.º 30171 de los delitos informáticos contra el patrimonio, conocer si estas, están reguladas de manera suficiente para garantizar su eficacia. La mayoría de los entrevistados señalan que el artículo 8º de la ley nº 30171 de los delitos informáticos contra el patrimonio, no está regulado de manera

suficiente para garantizar su eficacia, Montesinos, señala que esta ley no está regulada de acorde al haber devenido en el tiempo , y que los nuevos cambios tecnológicos en la informática han dado pies a los agentes tecnológicos actúen en la forma deliberada e ilegítimamente contra el patrimonio de los particulares y del estado, y al no estar regulada de manera adecuada y al encontrar vacíos legales en este artículo ya antes mencionado, los operadores de justicia se ven en la imposibilidad de sancionar eficazmente a estos ciberdelincuentes puesto que ellos solo pueden hacer lo que se les ha atribuido expresamente, ejerciendo la discrecionalidad únicamente cuando es aplicable.

Por otro lado, el entrevistado Cerón. (2022), señala, Si bien es cierto la ley 30096 tenía algunos vacíos, éstas fueron modificadas por la Ley 30171, ley que cumple a cabalidad para garantizar eficacia frente a los delitos que vulneren el artículo 8º sobre los delitos informáticos contra el patrimonio.

Ahora respecto a la segunda interrogante asociado al objetivo específico 1**,** de cómo se podría corregir los vacíos legales de nuestra normativa con respecto a los delitos informáticos contra el patrimonio, la gran parte de los entrevistados indican que se debería dar iniciativa legislativa, así tener modificaciones que permitan aplicar las normas de manera eficiente para cada caso en concreto, y del mismo modo a través de la modificación o derogación de nuestra normativa legal vigente según corresponda. Aunque el entrevistado Cerón. (2022), tiene una perspectiva diferente, al señalar que la ley 30096 sí tenía algunos vacíos, y que fueron subsanadas con la Ley 30171, por ello, esta ley sí garantiza los actos que vulneren los delitos informáticos contra el patrimonio.

En cuanto a tercera interrogante asociado a objetivo específico 1, cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio la mayoría de los entrevistados, Coaguila, Balcázar, Tohalino, Montesinos, Zambrano. (2022), sostienen que otras fuentes aplicadas son las doctrinas y las jurisprudencias. Así mismo el entrevistado Cerón. (2022), señala que, ante la existencia de vacíos, existen algunas fuentes aplicables al derecho, para poder sancionar a quienes cometan delitos informáticos y entre estas fuentes tenemos los tratados internacionales, constituciones, leyes y reglamentos.

Respecto a la primera interrogante asociado al objetivo específico 2 que busca conocer las modalidades más usuales o comunes para cometer delitos informáticos por los delincuentes cibernéticos. , La mayoría de los entrevistados coinciden que las modalidades de delitos informáticos más comunes y denunciados en nuestro país, están asociados a los fraudes informáticos, las estafas virtuales, y las suplantaciones de identidad, todos estos forman parte de lo que denominamos “ciberdelincuencia”, es muy usual la manipulación de dispositivos tecnológicos, contra sistemas de procesamientos de datos, sustracción de software y sabotaje informático, también tenemos el phishing y el pharming con la ejecución de operaciones bancarias, ambos entendidos dentro de los fraudes informáticos.

Resaltando el aporte de los entrevistados Tohalino y Suarez. (2022). quienes señalan; las modalidades más comunes son: el fraude informático, estafa y defraudaciones, que guardan un nexo para la comisión de otros delitos, como el hurto; cuando se comete una apropiación de dinero a través de sistemas informáticos

En cuanto a la segunda interrogante asociado al objetivo específico 2 que busca conocer, qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio, según la experiencia de los entrevistados. La mayoría refieren que los daños causados están asociados a la afectación del material y patrimonial; entendiendo que los datos informáticos en la mayoría de casos son medios o herramientas que permiten un fin lucrativo, por tanto, la manipulación, alteración, sustracción o destrucción de estas ocasionará la alteración de dicho fin, conllevando a sí, a una afectación del patrimonio, el entrevistado el Dr. Balcázar, (2022) señala a la afectación material entendido como valor económico”

Respecto a la tercera interrogante asociada al objetivo específico 2 que busca conocer, si existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico. Existen otras modalidades no contempladas explícitamente el artículo 8 de la ley N° 30171, Los entrevistados. Montesinos, Coaguila, Tohalino, Montesinos, Cerón y el resto, coinciden con las modalidades de defraudación, sabotaje, dentro de ello destacamos una modalidad señalada por el entrevistado. Vizcarra Pacheco.

(2022), quien menciona “el intrusismo, que refiere a valiéndose de los medios informáticos para la alteración y falsificación de títulos profesionales electrónicos y servicios.

DISCUSIÓN

Mediante el supuesto general se acentuó, que la intervención del Estado Peruano para tratar los delitos informáticos contra el patrimonio es deficiente, a causa de normas no acordes a la actualidad por los cambios de los últimos años a consecuencia de la COVID 19 y el avance tecnológico, creando así la necesidad de una intervención constante por parte del Estado teniendo en cuenta el elevado margen estadístico en estos últimos años.

En ese sentido, Viscarra (2022), señala la necesidad de una observación normativa a causa de los cambios dado por la pandemia y altos índices de la criminalidad informática contra el patrimonio. para constatar dichas causas mencionadas por Viscarra, recurriremos al informe de la ORACE (Oficina de racionalización y estadística) enviado a la OFAEC (Oficina de Análisis Estratégico contra la Criminalidad) del Ministerio Público y Fiscalía de la Nación; donde efectivamente dan a conocer que al año 2020, los delitos informáticos contra el patrimonio cubren el 42% del total general de delitos informáticos.

A si mismo Vizcarra (2022), también menciona que no tan solo basta con tratar y analizar la norma, sino que mediante la intervención del Estado Peruano se debería brindar alcances a los ciudadanos, en cuanto a la falta de educación sobre las amenazas informáticas, concientización y poca alfabetización digital, sustento que según el reporte de ciberseguridad 2020 del BID y OEA Riesgos, Avances y el Camino a seguir en América Latina y el Caribe, el Perú aún no cuenta con una estrategia nacional de seguridad cibernética.

Montesino (2022), señala; para que el Estado enfrente a la llamada criminalidad informática, los tipos penales tradicionales sean revisados y actualizados a través de un nuevo estudio y análisis correspondiente, accionando una serie de controles necesarios para su afrontamiento, teniendo en cuenta que estos delitos se desarrollan en un espacio abstracto; como es el Ciberespacio que traspasa fronteras mediante el uso y avance de la tecnología.

Con fin de conocer que dé cierto es lo dicho por el entrevistado, recurriremos a estudiosos donde, según Miró (2013) citado por la (OFAEC, 2020), detalla “delito informático; como todo acto delictivo que se desarrolla en el Ciberespacio, con las singularidades criminológicas, victimo lógicas y riesgo penal proveniente de ello dejando fuera del espacio físico tradicional” (p.13).

Huaytalla (2022), señala que este avance tecnológico influye; ya que al ser un agregado de conocimientos técnicos que permite crear, modificar y así adaptar nuestro entorno facilitando las actividades del hombre, siendo prescindible la presencia física, convirtiéndose así en los medios del cual se vale el sujeto activo, para no ser descubierto. Por lo tanto, las normas y procedimientos también deben ser adecuadas a los cambios de estos últimos años a causa de la pandemia.

A fin de sustentar lo dicho por Huaytalla recurriremos al derecho comparado tomando como ejemplo, legislaciones de países vecinos como Chile, que a causa del incremento de delitos informáticos por la llegada de la COVID 19, recientemente reformaron su ya existente legislación especial, Ley N°19223, el 22 de marzo del 2022 se aprobó el Boletín 12 192-95, que actualizó la ley N° 19223 que contenía 4 artículos, reformando y adecuando dicha Ley a la realidad actual de su sociedad pos pandemia, constando ahora de 21 artículos.

Por otro lado, y en sentido opuesto Cerón (2022), discrepa con la idea de los demás entrevistados, menciona que el Estado peruano debe intervenir; pero no en temas de regulación normativa, ya que la ley de los delitos informáticos contra el patrimonio si están reguladas acorde a nuestra realidad. Sino más bien en temas relacionados a la falta de capacidad de los operadores de justicia para interpretar y aplicar la norma de manera adecuada, la Ley N° 30096 fue modificada por la Ley N° 30171 e incorporó una serie de delitos informáticos dentro de los que se encuentran, la interceptación de información, suplantación de identidad, entre otros, con sus respectivas sanciones. Para sustentar lo dicho por Cerón, recurriremos al informe dado por el Ministerio Público Fiscalía de la Nación, Oficina de Análisis Estratégico contra la Criminalidad (OFAEC, 2020, p. 14). señala:

El año 2014, el Perú solicita formar parte del convenio de Budapest, el Consejo Europeo aprobó la solicitud el 2015. Para el 12 de febrero de 2019, el Congreso

de la República aprueba dicho Convenio, mediante Resolución Legislativa N° 30913 ratificado, por el Poder Ejecutivo, mediante D. S. N° 010-2019-RE, del 09 de marzo de 2019, estableciéndose el día 01 del 12 de 2019 como fecha de entrada en vigor. Así actualizando nuestra legislación a los artículos del convenio de Budapest, dentro de ello el capítulo v delitos informáticos contra el patrimonio artículos 8 de la Ley N° 30096, y modificatoria ley 30171.

reforzando dicha idea, Huaytalla (2022), también menciona que se debe enfatizar en trabajar sobre los procedimientos penales, que dificultan la investigación y enjuiciamiento ya sea; por desconocimiento de los agentes para tratar y obtener pruebas digitales, escasez de logística pericial, o dificultad para identificar al autor del delito.

En cuanto a la discusión asociado al objetivo General, a consecuencia de las distintas posturas de los entrevistados especialistas en el tema, basados en sustentos doctrinarios, estadísticos, derecho comparado, entre otras fuentes, nuestra postura como autores de la presente investigación; en cuanto a la intervención del Estado Peruano para tratar y prevenir los delitos informáticos contra el patrimonio, creemos que no es muy eficiente, ya que en los últimos tres años se ha generado cambios abruptos a consecuencia del aislamiento social por la COVID 19 situación que cambió nuestro modo de hacer nuestras actividades siendo necesario el uso de la tecnología, para trabajar, estudiar, realizar nuestros pagos compra entre otras cosas desde casa y con ello el incremento de los delitos informáticos, especialmente contra el patrimonio, como bien lo muestra la OFAEC (Oficina de Análisis Estratégico contra la Criminalidad) del Ministerio Público y Fiscalía de la Nación; donde efectivamente dan a conocer que al año 2020, los delitos informáticos contra el patrimonio cubren el 42% del total general de delitos informáticos y el reporte de ciberseguridad 2020 del BID y OEA Riesgos, Avances y el Camino a seguir en América Latina y el Caribe, el Perú aún no cuenta con una estrategia nacional de seguridad cibernética. Conociendo que el Perú no tiene ningún proyecto recientemente a fin de al menos discutir; si es necesario someter a análisis la norma asociada a los delitos informáticos contra el patrimonio siendo este el núcleo duro de la criminalidad en la actualidad con un 42%.

Si bien es cierto que el 30 de diciembre del 2020 por Resolución N° 1503-2020-MP-FN, se implementó una fiscalía especializada, con plataforma pericial a fin de mejora, creemos que esto no es suficiente, ya que como ejemplo tenemos al aporte de Chile quienes recientemente el 2022 reformaron su legislación de delitos informáticos para adecuarlo a la nueva realidad pos pandemia y así hacer frente a la nueva realidad. Con ello concordando con las ideas de los entrevistados Viscarra, Montesinos y otros.

A partir de los hallazgos encontrados respecto al análisis de la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio, aceptamos que el artículo 8º de la ley nº 30171 de los delitos informáticos contra el patrimonio no están reguladas de manera suficiente para proteger el patrimonio de las personas a quienes se les ha vulnerado, esta ley no se encuentra regulada de acorde a nuestra realidad social en que vivimos, si bien es cierto con la aparición del COVID 19, los casos de delitos informáticos contra el patrimonio han subido en índices jamás visto, las leyes peruanas no han complementado sus artículos y mucho menos han detallado cada nueva modalidad de los delitos cibernéticos contra el patrimonio; del mismo modo estos resultados guardan relación con lo que sostiene el entrevistado Montesinos (2022), que esta ley no está regulada de acorde al haber devenido en el tiempo , y que los nuevos cambios tecnológicos en la informática han dado pies a los agentes tecnológicos en la forma deliberada e ilegítimamente del patrimonio de los particulares y del estado, y al no estar regulada de manera adecuada y al encontrar vacíos legales en este artículo ya antes mencionado, los operadores de justicia se ven en la imposibilidad de sancionar eficazmente a estos ciberdelincuentes, puesto que ellos solo pueden hacer lo que se les ha atribuido expresamente, ejerciendo la discrecionalidad únicamente cuando es aplicable. Ello también es acorde con lo señalado por Cortés, Ballén y Duque (2015) quienes concluyeron, que los medios con los que cuenta el Distrito judicial de Villavicencio son escasos lo que reflejó ineficacia ante las situaciones de denuncias por delitos informáticos. Del mismo modo se prevalece concordancia con lo señalado por la INTERPOL (2017), el cual señaló que la ciberdelincuencia es un fenómeno sin fronteras, y ante ello, los organismos encargados de su regulación mediante la aplicación de sus leyes tienen problemas para hacerlo eficazmente; puesto que sus investigaciones tienen límites

transfronterizos haciéndolos ineficaces frente a los problemas de tipo jurídico y la diversidad de sus capacidades en el mundo. Así mismo, respecto al derecho comparado sobre las legislaciones de los Delitos informáticos de otros países, estos resultados guardan relación con Brasil, donde su legislación no cuenta con una Ley especial fuera del código penal, todo ello haciéndolo ineficaz ante la lucha contra los ciberdelitos. Sin embargo, hay una discordancia con lo señalado por el entrevistado Cerón (2022), quien sostiene que si bien es cierto la ley 30096 tenía algunos vacíos, éstas fueron modificadas por la Ley 30171, ley que cumple a cabalidad para garantizar eficacia frente a los delitos que vulneren el artículo 8º sobre los delitos informáticos contra el patrimonio, además sostiene que son los operadores de justicia quienes no están realizando un trabajo adecuado, y Cerón fundamenta su teoría, plasmando lo señalado por Carrera, Quilligana, Aguilar y Fiallos (2019), quienes concluyeron mediante un artículo de investigación que lleva por título Desafío de la ciberseguridad ante la legislación penal ecuatoriana., que tuvo como objetivo establecer punto de controversia respecto a casos de ciberdelitos, sobre la seguridad y el espacio y la intervención de la norma ante los delitos informáticos, llegando a determinar que se encontró los inconvenientes que suscita a la inseguridad a causa de los ciberdelitos ante la evidente situación de las normas ecuatorianas referente a este tipo de delitos debido a la falta de conocimiento de los magistrados y autoridades en cuanto al punto de vulnerabilidad de los organismos judiciales. Respecto a la postura de Cerón, nosotros estamos relativamente en desacuerdo, puesto que al estudiar y analizar la ley 30171, al obtener las respuestas de los entrevistados, al realizar el análisis de las doctrinas , expedientes, a la información de las fuentes estudiadas y al análisis del derecho comparado, sostenemos que las leyes peruanas respecto a los delitos informáticos contra el patrimonio son bastante pobres, porque sus leyes; específicamente la Ley 30171 en su artículo 8, regulan los delitos contra el patrimonio de manera general y no especifica cada modalidad que se ha presentado con la aparición del COVID 19 en adelante, en donde muchas personas se han visto obligados a usar las redes sociales y los medios de comunicación virtuales para todo tipo de acciones en su vida cotidiana, permitiendo que los ciberdelincuentes tengan la oportunidad de delinquir contra sus patrimonios, entonces al no estar bien detallado este artículo 8, no son

sancionados como deberían serlo; además señalamos que los magistrados si deberían ser capacitados o realizar capacitaciones respecto al uso adecuado de la tecnología acorde con nuestra realidad social en el ámbito de los ciberdelitos, es indiscutible que los ciberdelincuentes siempre están un paso delante de la ley y por tanto los magistrados necesitan y deben dominar el uso adecuado de las herramientas tecnológicas, y es una realidad que muchos magistrados peruanos tienen dificultades para utilizar adecuadamente las herramientas tecnológicas que prevalecen hoy en nuestros días; y lo fundamentamos señalando a La INTERPOL (2017),quien mencionó, que la ciberdelincuencia es un fenómeno sin fronteras, y ante ello, los organismos encargados de su regulación mediante la aplicación de sus leyes tienen problemas para hacerlo eficazmente; y no solo porque los operadores de justicia tienen dificultades para sancionar de manera adecuada a los ciberdelincuentes, sino también por quienes no están realizando un trabajo adecuado, puesto que sus investigaciones tienen límites transfronterizos haciéndolos ineficaces frente a los problemas de tipo jurídico y la diversidad de sus capacidades tecnológicas en el mundo.

Con lo que respecta a la discusión de los resultados de la investigación del análisis sobre el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades, la mayoría de los entrevistados coinciden que con la aparición del COVID 19, se dieron nuevas modalidades de delitos informáticos y éstas se encuentran asociados a los fraudes informáticos, sabotaje, chantaje, coacción, las estafas virtuales, y las suplantaciones de identidad. Y guarda similitud con lo sostenido por los entrevistados Tohalino y Suarez. (2022). quienes sostienen que las modalidades más comunes son: el fraude informático, estafa y defraudaciones, que guardan un nexo para la comisión de otros delitos, como el hurto; cuando se comete una apropiación de dinero a través de sistemas informáticos. De igual manera, Sobre otras modalidades de delitos informáticos contra el patrimonio, Pardo (2018) mencionó que específicamente dentro de cada tipo de delitos se podría identificar otras subcategorías de delitos, por lo tanto, dentro de delitos cibernéticos o informáticos contra el patrimonio podemos identificar al hurto, fraude, estafa y los sabotajes informáticos. Argentina también guarda concordancia sobre el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades, donde su legislación sobre los

delitos informáticos contra la propiedad señala como otras modalidades la estafa, defraudación y Daño informático. En cuanto a la existencia de otras modalidades, el país de Chile también señala de manera concordante la existencia de conductas lesivas contra el patrimonio, tales como: ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita, ataque a la integridad de los datos informáticos, falsificación informática, receptación de datos, fraude informático y el abuso de dispositivos. Por otro lado, Leyva (2021) también indica la presencia de otras modalidades de delitos informáticos que van en contra de las leyes, siendo realizados a través de sistemas de procesamiento de datos, contra la información digital siempre en perjuicio de una persona, que podría ser natural o jurídica, donde una de sus características es ser pluriofensivo toda vez que puede ser realizado mediante estafas, defraudación de patrimonio, la intimidad, la seguridad pública e informática. Respecto a otras modalidades de delitos informáticos, nosotros compartimos concordancia que si existen otras muy usadas por los ciberdelincuentes para cometer estos actos ilícitos; y lo fundamentamos con lo sostenido por Ruiz (2018) quien mencionó que la innovación tecnológica ha causado el origen de nuevos fraudes donde por medio de la informática o través del uso de la ingeniería informática , se manipulan los sistemas para delinquir contra el patrimonio de las personas permitiendo así el hurto, fraude, estafa y los sabotajes informáticos; así mismo es importante mencionar que una de las modalidades más usadas en nuestro país es el empleo del virus troyano, conocido mundialmente como Ransomware, aplicados siguiendo parámetros prefijados de navegación web, el cual se activa permitiendo el bloqueo del equipo informático y encriptando todos sus contenidos delinquiendo y perjudicando así a sus víctimas. Por ello, nuestro ordenamiento jurídico peruano necesita ser complementado específicamente en la Ley 30171 en su artículo 8; nuestra realidad social señala que en los últimos 3 años han aparecido nuevas modalidades de delitos informáticos, y éstas necesitan tener un tratamiento especial y específico para cada modalidad, que no está regulada en la mencionada ley. Una vez complementada la Ley 30171, nuestros operadores de justicia, ya previamente muy bien capacitados, tendrán las herramientas adecuadas para una acción eficaz y hacer frente a estas nuevas modalidades de los delitos informáticos contra el patrimonio y sancionar eficazmente a quienes cometan estos ciberdelitos.

V. CONCLUSIONES

Con respecto al análisis de la intervención del Estado Peruano para afrontar los delitos informáticos contra el patrimonio, concluimos que es poco eficiente debido a la poca y desactualizada actuación en su mayoría realizadas hasta el 2020, a fin de afrontar este .tipo de delitos, toda vez que en estos tres últimos años se ha generado muchos cambios en nuestra vida social a causa de la pandemia por la COVID 19, más el avance de la tecnología, a esto se suma el elevado porcentaje de uso de la tecnología por la sociedad, al realizar sus actividades diarias, llevado entre desconocimiento y errores, siendo puntos vulnerables y victimas para los sujetos activos del delito, reflejándose así altos márgenes estadísticos que muestran la cantidad de denuncias en el 2020 contra delitos informáticos contra el patrimonio llegando a un 42% mediante el reporte de la OFAEC del total de delitos informáticos, en este sentido es preocupante la realidad actual tomando en cuenta los factores antes mencionados, nos vemos en la necesidad, de que el Estado Peruano debe actualizar acciones a fin de afrontar y dar la importancia que amerita.

Con respecto al análisis de la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio, en opinión de los magistrados entrevistados, las fuentes estudiadas, doctrinas, expedientes y derecho comparado, se concluyó, que el artículo 8º de la ley Nº 30096 de los delitos informáticos contra el patrimonio es poco eficiente al no encontrarse regulado de manera suficiente, siendo genérica en su redacción, faltando especificaciones en su contenido, además esta ley no se encuentra regulada acorde a nuestra realidad social en que vivimos, con la aparición del COVID 19 los casos de delitos informáticos contra el patrimonio han aumentado, a esto se suma la falta de recursos logísticos periciales, capacitaciones constantes a los operadores de justicia. Ha diferencia de la legislación de Chile que recientemente mediante Boletín 12 192-95, se actualizo a una nueva Ley N°21459, el 20 de junio del 2022, reestructurando el cuerpo legal de los delitos informáticos por los cambios a consecuencia de la pandemia por COVID 19.

Con lo que respecta al análisis, sobre el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades, rescatando los aporte de los entrevistados especialistas en el tema, las fuentes estudiadas, doctrinas, expedientes y derecho comparado, se concluyó que estas no estan

especificadas en el artículo 8 de la Ley 30096, ya que con la aparición del COVID 19, se dieron nuevas modalidades de delitos informáticos y dentro de cada tipo de delitos se podría identificar otras sub categorías de delitos donde podemos identificar a los fraudes informáticos, espionaje, intrusismo, chantaje, las estafas virtuales, y las suplantaciones de identidad. Como se observaba en los artículos derogados (207-A, 207-B, 207-C, 207-D) del capítulo X de los delitos informáticos del Código Penal donde se podía distinguir algunas modalidades especificadas.

VI. RECOMENDACIONES

Primero, el Estado peruano a través del presidente de la Republica y los congresistas, deberían generar iniciativa legislativa mediante proyectos de Ley que busquen poner sobre mesa de estudio el artículo 8 de la Ley 30096 y modificatoria Ley 30171 a fin de analizar tanto la estructura sustantiva como procedimental la cual tiene que ser acorde a nuestros tiempos y realidad social, teniendo en cuenta los cambios ocasionados por la Pandemia COVID 19,

Segundo En cuanto a la eficacia legislativa el Estado, mediante el poder judicial, fiscalías, y otros entes jurisdiccionales deben brindar capacitaciones muy seguidas y constantes de carácter obligatorio para los operadores del derecho; respecto a nuevas modalidades de delitos informáticos contra el patrimonio que prevalecen en nuestros días y el uso adecuado de las herramientas tecnológicas, adicional a ello Implementar inversión en recursos logísticos periciales en distintos puntos del país, para así facilitar la accesibilidad por parte de los operadores de justicia. Por ejemplo: plataformas periciales y adquisición de software conocido como llaves digitales para acceso y desbloque de programas y dispositivos tecnológicos.

Tercero, en vista que se vienen presentando nuevas modalidades de delitos informáticos en nuestra sociedad, es importante que nuestro ordenamiento jurídico peruano contenga incisos en el artículo 8 de la Ley 30096 que permita especificar y distinguir los tipos penales en cuanto a sus modalidades; para que los operadores de justicia puedan contar con una mejor y clara descripción sustantiva de la norma y así aplicar una mejor interpretación, podríamos considerar en adicionar estos incisos:

Espionaje informático: El que espié maliciosamente para obtener información confidencial o secreta a través de los datos informáticos contenidos un sistema de tratamiento de información.

intrusismo informático: El que mediante uso de sus conocimientos, experiencia y habilidades informáticas viola las medidas de seguridad de un sistema de datos

Chantaje informático: El que se apropie de la información de un hecho confidencial mediante un sistema de procesamiento de datos a fin de obtener un beneficio, a cambio del silencio a no revelar la conducta cuya divulgación podría perjudicarlo.

REFERENCIA

Aroni, N. y Barrios, R. (2018). *Análisis de los principales factores financieros, operacionales y de reputación empresarial que vienen siendo impactados por el incremento de los delitos informáticos en los principales bancos del Perú como son Banco de crédito del Perú y Banco Continental en los últimos 5 años.* https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625668/Aroni_cn.pdf?sequence=1&isAllowed=y

Ashikin, K. et al. (2017). *Security Strategies for Hindering Watering Hole Cyber Crime Attack.* https://reader.elsevier.com/reader/sd/pii/S1877050917329708?token=69E892C53697469487D24DF3059586F6F3F4412AFDFC89ECFE544223621157FFE04B72C887776106944280628A2F4D30&originRegion=us-east-1&originCreation=20211123013820

Carrera, C., Joel, E., Quilligana, B., Aguilar, M. y Fiallos, B. (2019). Desafío de la ciberseguridad ante la legislación penal. *Revista Dilemas Contemporáneos: Educación, Política y Valores.* https://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=12&sid=880ae87b-8e0d-4ebf-8f9e-4d91b3f5093b%40sessionmgr4007

Cascavilla, G. et al. (2020). *Cybercrime threat intelligence: A systematic multi-vocal literature review.* https://reader.elsevier.com/reader/sd/pii/S0167404821000821?token=681C6D8D7F27A62FCD5E317C9BD9B8F4D7B2E31E98E195ABEB46EB538AD2EC219078E4C42E71DC20749AC51FDBF09147&originRegion=us-east-1&originCreation=20211120184244

Cconislla, R. (2017). *Incorporar la modalidad del delito de pedofilia en la Ley Nº 30096 capítulo III de los delitos informáticos.* *https://repositorio.uandina.edu.pe/handle/20.500.12557/946*

Cortés Borrero, R., Ballén Rojas, J. A., Duque Montes, J. J. (2015). La persecución judicial contra los delitos informáticos en el Distrito Judicial de Villavicencio. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías. Universidad de*

los Andes Colombia).https://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=4&sid=880ae87b-8e0d-4ebf-8f9e-4d91b3f5093b%40sessionmgr4007

Chávez, R. (2018). *EL DELITO CONTRA DATOS Y SISTEMAS INFORMÁTICOS EN EL DERECHO FUNDAMENTAL A LA INTIMIDAD PERSONAL EN LA CORTE SUPERIOR DE JUSTICIA DE LIMA NORTE, 2017*. http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y

Corte Suprema de Justicia, Sala de Casación Penal, Sala de Decisión de Tutelas n° 1, STP6279-2017, 4 de mayo de 2017. https://cortesuprema.gov.co/corte/wp-content/uploads/not/penal17/avisos/stp6279%20-%2091612.PDF

División de Investigación de Delitos de Alta Tecnología DIVINDAT (2019). *Estos son los delitos informáticos más frecuentes en el Perú según la Policía*. https://andina.pe/agencia/noticia-estos-son-los-delitos-informaticos-mas-frecuentes-el-peru-segun-policia-781320.aspx

Díaz Herrera, C, (2018). Investigación cualitativa y análisis de contenido temático. *Orientación intelectual de revista Universum Revista General de Información y Documentación ISSN: 1132-1873*. http://dx.doi.org/10.5209/RGID.60813

Elvis, E. (2017) *"La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017.*http://repositorio.unsa.edu.pe/handle/UNSA/6436

García, V. (2019). Cómo está avanzando la ciberseguridad en el Perú breve aproximación al marco normativo. *Revista de Actualidad Jurídica Uría Menéndez*. file:///C:/Users/belin/Desktop/jhon/PROYECTO%20DE%20INVESTIGACI%C3%93N/revistas%20indexadas/C%C3%93MO%20EST%C3%81%20AVANZANDO%20LA%20CIBERSEGURIDAD%20EN%20EL%20PER%C3%9A

Hancco, Z. (2017). *"La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017"* http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/6436/DEhazaey.pdf?sequence=1&isAllowed=y

Instituto Nacional de Estadística INEI (2019*). Anuario estadístico de la criminalidad y seguridad ciudadana 2012 - 2018*. https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1691/libro.pdf

Leyva, C. (2021). *Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales.* file:///C:/Users/sandra/Downloads/68634%20(1)%20(1).pdf

Leyva, C. (2021). *Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales*. file:///C:/Users/sandra/Downloads/68634%20(1)%20(1).pdf

Lizandra, J., Y Peiró Velert, C. (2020). *Las relaciones sociales y su papel en la motivación hacia la práctica de actividad física en adolescentes: Un enfoque cualitativo.* Artículo issue España. *https://eds.s.ebscohost.com/eds/pdfviewer/pdfviewer?vid=16&sid=5a2d0c9f-e144-4c3c-84d8-57b56327c7c8%40redis*

Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Revista Ius et Praxis*. https://eds.s.ebscohost.com/eds/detail/detail?vid=5&sid=ec5c4312-243d-449a-ab7b-1cb0541ea4f0%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=134791161&db=fua

Ley 12737 de 2012. (2012, 30 de noviembre) Republica de Brasil. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Ley 1768 de 1997. (1997) Republica de Bolivia. https://www.oas.org/juridico/spanish/gapeca_sp_docs_bol1.pdf

Ley 30171 de 2014. (2014, 10 de marzo) Congreso de la Republica de Perú. Diario Oficial N° 518568. https://www.leyes.congreso.gob.pe/Documentos/Leyes/30171.pdf

Mayer L., L. (2017). *El bien jurídico protegido en los delitos concursales.* Valparaíso, Chile. https://www.proquest.com/docview/2002988563/fulltextPDF/8DE223D88EFB469BPQ/3?accountid=37408

Mayer, L. (2016). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. Universidad de Talca. *Revista Ius et Praxis.* https://scielo.conicyt.cl/pdf/iusetp/v24n1/0718-0012-iusetp-24-01-00159.pdf

MAYER, L. (20I7). El bien jurídico protegido en los delitos informáticos, la funcionalidad informática como interés que surge respecto de redes computacionales*. Revista chilena de derecho. Vol. 44(1),7.* http://dx.doi.org/10.4067/S0718-34372017000100011

MAYER, L. (20I7). El bien jurídico protegido en los delitos informáticos, tutela de un bien jurídico especifico y común a todos los delitos informáticos. *Revista chilena de derecho. Vol. 44(1),3.*

http://dx.doi.org/10.4067/S0718-34372017000100011

Martínez, M. (2020). *Ciberdelitos traen una batalla sin descanso a empresas y autoridades en Perú.* https://www.proquest.com/docview/2365129046/EE0A93976E134FC0PQ/9?accountid=37408

Martínez S., Murillo M. y Sánchez V. (2020). Desafío del sistema penal salvadoreños en la aplicación de la ley especial contra los delitos informáticos y conexos*. Repositorio Institucional, Universidad de El Salvador.* https://eds.a.ebscohost.com/eds/detail/detail?vid=7&sid=f2cd81f4-cfdc-43a3-bb17-

6e2061d604d0%40sessionmgr4006&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=edsbas.F76EF066&db=edsbas

MINISTERIO PUBLICO. (2019). *Boletines estadísticos del Ministerio Público 2019 Ley 30096.* https://www.mpfn.gob.pe

Ministerio Público Fiscalía de la Nación, Oficina de Análisis Estratégico contra la Criminalidad OFAEC (2020). *Informe de Análisis N°04 Ciberdelincuencia: pautas para una Investigación Fiscal Especializada.* https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERU%CC%81%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIO%CC%81N%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Nizama, M., y Nizama, L. (2020). EL ENFOQUE CUALITATIVO EN LA INVESTIGACIÓN JURÍDICA, PROYECTO DE INVESTIGACIÓN CUALITATIVA Y SEMINARIO DE TESIS. *Revista Vox Juris. Nbr. 38-2, July 2020.* http://vlex.com.pe/vid/enfoque-cualitativo-investigacion-juridica-846600927

Octavio I. (2018). ciberseguridad errores y omisiones y lo que falta. *editorial CISA comunicación e información, S.A. de C.V.* https://go.gale.com/ps/retrieve.do?tabID=T003&resultListType=RESULT_LIST&searchResultsType=SingleTab&hitCount=5&searchType=AdvancedSearchForm&currentPosition=3&docId=GALE%7CA550168652&docType=Article&sort=Relevance&contentSegment=ZSPS&prodId=IFME&pageNum=1&contentSet=GALE%7CA550168652&searchId=R3&userGroupName=univcv&inPS=true

Okutan, A. (2019). *A Framework for Cyber Crime Investigation.* https://reader.elsevier.com/reader/sd/pii/S1877050919312141?token=AACE97376657E4B89298C592AFC629C71D7E6CDE6ADC4DED5836E51B204AE5A15BF7EAA5C090DA3A4728755EF21D1F07&originRegion=us-east-1&originCreation=20211123004431

Organización de los Estados Americanos OEA (2022). *Portal Interamericano de Delitos Cibernéticos.* http://www.oas.org/es/sla/dlc/cyber-es/desarrollo-pais.asp

Pardo, V. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.* file:///C:/Users/belin/Desktop/jhon/PROYECTO%20DE%20INVESTIGACI%C3%93N/Pardo_VA%20Tratamiento%20jur%C3%ADdico%20penal%20de%20los%20delitos%20inform%C3%A1ticos.pdf

Patil, R. & Devane, S. (2019). *Network Forensic Investigation Protocol to Identify True Origin of CyberCrime.* https://reader.elsevier.com/reader/sd/pii/S1319157819311103?token=6AEAF3ECF33CE50B89286533871DD56D62528F72DBB030E3A6DFD06AE86CBA50BF72653A1EF6B466B7C9EF54412429F8&originRegion=us-east-1&originCreation=20211123035248

Pardo, V. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.* file:///C:/Users/belin/Desktop/jhon/PROYECTO%20DE%20INVESTIGACI%C3%93N/Pardo_VA%20Tratamiento%20jur%C3%ADdico%20penal%20de%20los%20delitos%20inform%C3%A1ticos.pdf

Pythagoras, N. (2021). Misinformation, disinformation, and fakenews*: Cyber risks to business.* https://reader.elsevier.com/reader/sd/pii/S000768132100135X?token=ABE94DE7988F9AA307C56C7A336E4579AE23D8D7A8F21D250BEF0B43EFFFB87D6075EE1F7867F81183312B07CAAF55B9&originRegion=us-east-1&originCreation=20211125163656

Rachana, P. & Devane, Y. (2020). Backtracking Tool Root-Tracker to Identify True Source. *of Cyber Crime. Revista.* https://reader.elsevier.com/reader/sd/pii/S187705092031098X?token=4D99A5070E00EBBE3A26566B89639BF1345BA4643E4B38D4F5B6883228D1E17D052BA4343622B92E156557034320DD47&originRegion=us-east-1&originCreation=20211123011508

Ruiz de Valbuena, I. (2018). Las empresas se resisten a denunciar los ciberataques por miedo a las consecuencias en su reputación*. Revista Especial Directivos 1762.*

https://eds.p.ebscohost.com/eds/detail/detail?vid=5&sid=d3db769c-b6c5-4a9da5a47da2bc9c8d70%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZQ%3d%3d#AN=138879817&db=fua

Rodríguez, E. (2019). LA HERMENÉUTICA GADAMERIANA COMO SÍNTESIS ENTRE EL ENFOQUE CUANTITATIVO Y CUALITATIVO EN LA INVESTIGACIÓN SOCIAL. *Revista Interdisciplinaria de Filosofía y Psicología.* https://eds.s.ebscohost.com/eds/pdfviewer/pdfviewer?vid=6&sid=5a2d0c9f-e144-4c3c-84d8-57b56327c7c8%40redis

Tribunal Constitucional. Sentencia N°1100/2020, 10 de diciembre del 2020, f. j. 5°. https://tc.gob.pe/jurisprudencia/2020/01189-2019-HC.pdf

Vásquez, C. E., Regalado, J. M., y Guadron, R. S. (2017). *Cibercrimen e informática forense: introducción y análisis en El Salvador*. *Revista Tecnológica.* http://www.redicces.org.sv

Zevallos, P. (2020). *Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce?* https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/

ANEXOS

OBJETIVO GENERAL Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio				
Entrevistados		¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?	¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿Por qué?	Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?
1	Balcázar Chilcho, Jaime	El Estado debe usar tecnología de última generación a efectos de prevenir y sancionar las conductas ilícitas que afectan a los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la	Si influyó, porque en los últimos tiempos, se usa las transferencias de dinero, compras, ventas de producto, todo ello virtualmente, entonces la delincuencia se ha especializado a efectos de delinquir, robar y estafar, usando la identidad de las victimas a efectos de apoderarse de su patrimonio.	No está establecido claramente, en todo caso es necesario una mejor y clara tipificación de los delitos informáticos, toda vez que a raíz de la pandemia se han incrementado este tipo de delitos.

		información o de la comunicación con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.		
2	Coaguila Tapia, Percy	El estado debería accionar una serie de controles necesarios para resguardar la información cibernética e ir combatiendo estos delitos mediante la firme aplicación de todas las leyes que castigan a quienes los cometen.	Si, porque el uso de la informática a nivel mundial tiene una importancia relevante frente a la sociedad sobre todo para comunicarse, informarse y realizar movimientos económicos, y esto si influye en el incremento de estos delitos, permitiendo delinquir a los delincuentes.	No son reguladas acorde a nuestra realidad. Las medidas se confinamiento y el teletrabajo nos hacen ser más vulnerables a este tipo de delitos y el estado no está tomando en cuenta estos cambios tecnológicos en sus normas.
3	Montesinos Córdova, Clenin	El estado debería afrontar los delitos informáticos a través de una regulación eficaz de nuestra normativa penal, ello a través de un nuevo estudio y análisis	Si principalmente porque los agentes activos, valiéndose de sus conocimientos de la informática tienen a perjudicar a las víctimas para beneficiarse	No, en tanto que los cambios tecnológicos en la informática son constantes más aun después del factor COVID-19, en la que en todo ámbito particular y público se vale de la informática para el

		correspondiente a través de los organismos y entidades pertinentes dado el incremento de los comportamientos ilícitos constantes que sufren las personas particulares y el estado.	ilícitamente de sus bienes patrimoniales.	desarrollo de las actividades y sobre la cual en forma constante se producen comportamientos virtuales ilícitos por parte de los agentes activos que no se encuentran reguladas en la ley 30171 que fue publicada en el diario oficial el peruano, 10 de marzo del 2014.
4	Tohalino Alemán, Victor	En nuestro país nos encontramos con que el ordenamiento jurídico en materia penal. No ha avanzado en estos últimos tiempos a diferencia de otras legislaciones, por tanto, es necesario para enfrentar a la llamada criminalidad informática que los tipos peales tradicionales sean revisados, sean	Por supuesto, el avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamiento delictivos antes impensables y en algunos casos de difícil tipificación en las normas penales tradicionales.	No, efectivamente el desarrollo y masificación de las nuevas tecnologías de la información han dado lugar a cuestiones tales como análisis de la suficiencia del sistema jurídico actual para regular las nuevas posiciones, los nuevos escenarios, en donde se debate los problemas del uso y abuso de la actividad informática y su repercusión en nuestra realidad actual.

		actualizados para así consolidar la seguridad jurídica.		
5	Vizcarra Pacheco, Edgar	Es obligatorio del estado hacer frente a estos delitos que tiene un aumento significativo en estos tiempos de pandemia, por ello se debe tener una regularización eficaz en nuestra normativa penal, para poder disminuir y hacer frente las conductas antijuridicas de estos cibercriminales.	si, porque la falta de educación sobre las amenazas informáticas, concientización, la poca alfabetización digital y tendencia innata del ser humano a confiar, permitió que los atacantes se aprovechen y vulneren sus patrimonios.	No, a pesar de los cambios de nuestra sociedad, según el reporte de ciberseguridad 2020 del BID y OEA- Riesgos, Avances y el Camino a seguir en América Latina y el Caribe, el Perú aun no cuenta con una estrategia nacional de seguridad cibernética.
6	Cerón Salazar Nelson	El Estado peruano debería promover los convenios multilaterales que ayuden a disminuir los delitos informáticos, con ello tener la cooperación mutua con	Por supuesto que sí, y no solo en nuestro país, incluso en países con tasas de inseguridad muy bajas. El uso de la tecnología se ha convertido en uno de los principales factores que	Evidentemente nuestras leyes si están reguladas acorde a nuestra realidad, el problema se encuentra en la interpretación de estas leyes por parte de algunos colegas quienes por la falta de

		otros Estados para la persecución de estos delitos. Los ciberdelincuentes están un paso adelante sobre los ciudadanos y autoridades, por ello la importancia de la cooperación con los otros estados	ayudaron al incremento de los delitos informáticos contra el patrimonio.	capacitaciones en la cuestión informática, no aplican de manera adecuada la Ley 30171, la citada norma incorporó una serie de delitos informáticos, dentro de los que se encuentran interceptación de información, suplantación de identidad, entre otros, a estos tipos penales se les establecieron sanciones penales con la finalidad de contrarrestar su consumación, pero ya depende de los operadores de justicia aplicar las leyes correctamente.
7	Huaytalla Pillaca Guisella	Con la llegada de la COVID 19 y el avance tecnológico, el mundo ha dado un cambio de 360 grados, por ello el Estado en interacción de sus distintos órganos jurisdiccionales, deberían	Claramente si, influye de forma directa, partiendo de que la tecnología avanza constantemente, siendo un conjunto de conocimientos técnicos, que permite crear, modificar y así adaptar nuestro	A pesar de que nuestra legislación respecto a los delitos informáticos tuvo una reforma en el año 2014 mediante la ley 30171, sería importante evaluar ciertas actualizaciones, en cuanto nuevos posibles tipos penales

		someter a mesa estudio, revisar y analizar en busca de posibles deficiencias de la norma, en cuanto a su estructura sustantiva y procedimental, teniendo en cuenta que muchos de los procedimientos penales se dificultan en cuanto a la investigación y enjuiciamiento ya sea; por desconocimiento de los agentes para tratar y obtener prueba digitales, escasez de logística pericial, o dificultad para identificar al autor del delito.	entorno facilitando las actividades del hombre, siendo prescindible la presencia física de esta manera siendo el medio y camuflaje que utilizan los sujetos activos, para no ser descubiertos.	considerando estos 3 últimos años con la llegada de la COVID 19 y el confinamiento social, la Sociedad tuvo que adaptarse al uso de la tecnología, sin conocimiento adecuado, entre errores, siendo así vulnerables, facilitando la comisión de los delitos informáticos contra el patrimonio, que avanzan a pasos agigantados, valiéndose de nuevas formas y mecanismos para burlar a las autoridades y las normas, e incluso con la implementación de la nueva Fiscalía Corporativa Especializada en Ciberdelincuencia 2021, que es positivo, aun abría más que implementar.

8	Guerra Soto Cristhian Miguel	He podido reconocer ciertos quiebres sobre los cuales el Estado debería actuar, uno de ellos es la falta de conocimiento y capacitación, tanto de magistrados, fiscales, peritos, abogados y personal policial, entre otros. Segundo la falta de coordinación y comunicación, para trabajar en conjunto, no tan solo entre personal asociados al derecho sino la interacción con especialistas ya sean técnicos, ingenieros, especialistas en software.	Si influye, la tecnología hoy en día implica una necesidad para la vida del hombre, el avance de esta sin tener de tras un medio adecuado de contingencias para supervisar a quienes lo usan, lo ha convertido en un factor criminógeno que posibilita la vulneración de derechos a la privacidad e intimidad mediante el acceso a nuestras plataformas electrónicas privadas y así manipular y apropiarse de datos de información pudiendo estos tener valor económico como cuentas bancarias , proyectos, etc. y así afectar el patrimonio	En realidad, no son acordes, a mi parecer, la descripción de la norma asociada a los delitos informáticos contra el patrimonio es genérica con falta de especificaciones en cuanto al patrimonio privado entendido como un supuesto y falta especificar respecto a las formas.
9	Lucio Alfredo Zambrano Rodriguez	El Estado debería actuar en dos aspectos, uno de ellos es la falta de conocimiento y capacitación, tanto de	Si influye, la tecnología hoy en día implica una necesidad para la vida del hombre, el avance de esta sin tener de tras un medio	No son acordes, a mi parecer, la descripción de la norma asociada a los delitos informáticos contra el

		magistrados, Fiscales peritos, abogados y personal policial, entre otros. Segundo la falta de coordinación entre estos agentes que son pieza fundamental en todo el procedimiento.	adecuado de contingencias para supervisar a quienes lo usan, lo ha convertido en un factor criminógeno que posibilita la vulneración de derechos a la privacidad e intimidad	patrimonio es genérica con falta de especificaciones
10	Hinostroza Rodríguez Carlos	El Estado conjuntamente con sus distintos entes jurisdiccionales están obligados a tomar iniciativa frente a este nuevo tipo de delitos, como son los informáticos, como toda norma que no alcanza la eficacia jurídica que se busca, esta tiene que ser sometida a un profundo análisis, ante los entes especializados, incluso recurrir a profesionales	Si influye, la tecnología se ha vuelto indispensable con el pasar de los tiempos para las actividades de la sociedad, pues es este conocimiento de la informática que muy pocos conocemos y es de esta que se valen los agentes activos para la comisión de los distintos delitos informáticos y nuevos tipos criminógenos que hoy en día acontecen.	Considero que no son acordes. el desarrollo y extensión de las nuevas tecnologías de la información, han dado lugar a cuestiones tales como análisis en cuanto si es suficiente el sistema jurídico actual para regular las nuevas posiciones, los nuevos escenarios, y tipos delictivos.

		asociados al estudio de software que permitan comprender esta interacción, frente a esta nueva realidad tecnológica.		

OBJETIVO ESPECÍFICO 1 Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio				
Entrevistados		Según su experiencia laboral, ¿considera que el artículo 8º de la ley n.º 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?	¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?	¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?
1	Balcázar Chilcho, Jaime	No está regulado claramente, porque no se precisa el patrimonio privado, solamente	Corresponde al congreso de la república, legislar al respecto, o caso contrario los fiscales, y	Doctrina, la jurisprudencia, los acuerdos plenarios.

		se habla del patrimonio del estado de fines asistenciales.	jueces informar a efectos de hacer acuerdos plenarios al respecto.	
2	Coaguila Tapia, Percy	Esta ley no está regulada de manera eficiente, puesto que, con el transcurso de los días, el mundo ha sufrido cambios tecnológicos que dieron inicio e incremento para aquellos sujetos activos quienes aprovechan la tecnología para beneficiarse ilegítimamente del patrimonio de terceros.	Para corregir las lagunas o vacíos legales, se debería dar inicialmente legislativa, así tener modificaciones que permitan aplicar las normas de manera eficiente para cada caso en concreto.	La fuente principal de nuestro ordenamiento jurídico es la ley, adecuada al comportamiento humano, sin embargo, es muy necesario que se realice cambios en su contenido, debido a la varianza de nuestra sociedad, y el uso masivo de la tecnología.
3	Montesinos Córdova, Clenin	No esta regulada de manera suficiente al haber devenido en el tiempo nuevos cambios tecnológicos en la informática que precisamente han dado pies a los agentes tecnológicos quienes en estos últimos tiempos se	Atreves de la modificación o derogación de nuestra normativa legal vigente según corresponda.	Al ser herederos del sistema romano germánico, considero que la fuente principal para nuestro sistema jurídico penal es la ley, sobre la cual debe elegirse el comportamiento humano de los agentes activos de esta clase de ilirios penales, sin perjuicio de que

		aprovecharon de la virtualidad para beneficiarse en la forma deliberada e ilegítimamente del patrimonio de los particulares y del estado.		las mismas sean interpretadas valiéndose de las otras fuentes del derecho.
4	Tohalino alemán, Víctor	*No. La ley 30096 tenía algunos vacíos, los cuales fueron modificados con la ley 30171, sin embargo, como nuestra sociedad es cambiante, es necesario realizar modificaciones acordes a los delitos informáticos que se vienen cometiendo.	Al tener vacíos, se debe integrar el derecho, esto es, analizar el derecho como un todo, vero en la totalidad para buscar una solución ante la ausencia o insuficiencia de regulación para supuesto especifico.	Doctrinas y jurisprudencia.
5	Vizcarra Pacheco, Edgar	la ley N°30171, tiene algunos vacíos que deben ser subsanados los más pronto posible, los ciberdelincuentes muchas veces no pueden ser sancionados debido a estas.	Para subsanar estos vacíos es menester del estado, realizar modificaciones y derogar algunas normativas vigentes.	Principalmente se acude a las doctrinas y jurisprudencias.

6	Ceron Salazar Nelson	Sí, ya antes lo había mencionado. Si bien es cierto la ley 30096 tenía algunos vacíos, éstas fueron modificadas por la Ley 30171, ley que cumple a cabalidad para garantizar los delitos que vulneren el artículo 8º sobre los delitos informáticos contra el patrimonio.	Desde una perspectiva objetiva, la ley 30096 sí tenía algunos vacíos, y que fueron subsanadas con la Ley 30171, ley que sí garantiza los delitos que vulneren el artículo 8º sobre los delitos informáticos contra el patrimonio.	Ante la existencia de vacíos, existen algunas fuentes aplicables al derecho, para poder sancionar a quienes cometan delitos informáticos, entre estas fuentes tenemos los tratados internacionales, constituciones, leyes, reglamentos; así mismo están las doctrinas, la costumbre y los principios generales del derecho consagrados por la jurisprudencia.
7	Huaytalla Pillaca Guisella	La actual legislación artículo 8º de la Ley n.º 30171, carece de eficacia, en cuanto a la falta de expresión talvez de modalidades delictivas que constantemente innovan, anteriormente en el Código Penal artículo 186 inc.4 inciso derogado, refería al uso	Partiendo de un estudio y análisis minucioso de la norma regulada desde lo específico hacia lo genérico acorde a nuestra realidad social, mediante la iniciativa del Estado con la intervención de especialistas en el tema, tanto del derecho como especialistas de las ciencias	Debido a estas nuevas formas de delinquir basadas en conjeturas, poco familiarizadas o conocidas e en el entorno del derecho, basado en ello otras fuentes a recurrir seria la doctrina, jurisprudencia. Leyes internacionales.

		tecnología, transferencia electrónica como un agravante, creo yo que hoy en día debería tratarse los delitos informáticos en cuanto a sus modalidades teniendo en cuenta al hurto informático, sabotaje, estafa y otros.	tecnológicas ya que es necesario comprender la complejidad y funcionabilidad de aquel ciber espacio realidad donde se cometen específicamente estos tipos de delitos.	
8	Guerra Soto Cristhian Miguel	Para alcanzar la eficacia a mi parecer faltaría un análisis profundo de la norma para una adecuada redacción de los delitos informáticos contra el patrimonio, relacionados al artículo 8 de fraudes, considerando las conductas que normalmente se califican como tales, podrá constatarse que el término fraude informático es entendido de forma bastante más amplia y	Ello recae en los legisladores, ejecutivo y magistrados mediante el interés e iniciativa de poder poner en observación y análisis la norma asociada para así poder subsanar las falencias que se encuentren, e incluso tomar en cuenta las aportaciones o críticas constructivas de los distintos agentes asociados a estos casos, de delitos informáticos.	Doctrina, jurisprudencia y Leyes internacionales.

		que, en ese sentido, suelen incluirse comportamientos muy diversos.		
9	Lucio Alfredo Zambrano Rodriguez	Carece de eficacia en cuanto a la falta de expresión de las modalidades delictivas que constantemente innovan con el pasar del tiempo.	Partiendo de un estudio y análisis minucioso de la norma regulada desde lo específico hacia lo genérico acorde a nuestra realidad social, mediante la iniciativa del Estado con la intervención de especialistas en el tema.	Doctrina y jurisprudencia.
10	Hinostroza Rodríguez Carlos	No está regulada de manera eficiente, puesto que, con el transcurrir de los días, las sociedades han sufrido cambios tecnológicos, avances, que permitieron la creación de nuevos tipos delictivos asociados a la cibernética.	Para corregir los vacíos legales, primero dar iniciativa legislativa, en cuanto revisión y posibles modificaciones de la ley, que permitan aplicar las normas de manera eficiente.	Doctrina y jurisprudencia.

OBJETIVO ESPECÍFICO 2 Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades				
Entrevistados		¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernéticos?	De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?	¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?
1	Balcázar Chilcho, Jaime	Por intermedio de Hacker entran a la cuenta y se hacen pasar por la persona dueña de las cuentas, a efectos de apropiarse de dinero, haciéndose transferencias de dinero.	Apropiarse de dinero de las cuentas. Daños materiales entendido como valor económico afectando el patrimonio	Si hay modalidades que tienen que ser incluidas, y sancionadas en el código penal.
2	Coaguila Tapia, Percy	Fraude por la manipulación de computadoras contra un sistema de procesamientos,	He defendido casos de sabotaje informático y robo de servicios.	Si, entre las más frecuentes en nuestra sociedad son los robos de servicios y fraude informático.

		robo de software y sabotaje informático.		
3	Montesinos Córdova, Clenin	Atentado a los datos informáticos, interferencia telefónica, el fraude informático, entre otros.	No, he resuelto.	Si las mismas que podrían comprenderse dentro del ilícito penal de fraude informático.
4	Tohalino Alemán, Victor	Las modalidades más comunes son: el hurto, cuando se comete una apropiación de dinero a través de sistemas informáticos estafa y defraudaciones.	Estafa y defraudaciones. Con daño material asociado al perjuicio del patrimonio	Estafa y defraudación
5	Vizcarra Pacheco, Edgar	Los delitos informáticos que tienen mayor relevancia son los daños o modificaciones de programas o bases de datos, sabotajes, virus o gusanos. En este sentido el solo hecho de Hackear el ordenador de una persona se considera un delito.	Fraudes, cometidos mediante la manipulación de equipos informático y falsificaciones informáticas.	Si existe, y entre ellos debería ser visto con mayor protección el delito de intrusismo. Valiéndose de los medios informáticos para la alteración y falsificación de títulos profesionales electrónicos y así brindar servicios.

6	Cerón Salazar Nelson	Entre los delitos informáticos más comunes y denunciados en nuestro país son los fraudes informáticos, las estafas virtuales, y las suplantaciones de identidad, todos estos forman parte de lo que denominamos “ciberdelincuencia”, de acuerdo a las estadísticas que me ha tocado defender.	Me ha tocado defender muchos casos de Apropiación ilícita de dinero de las cuentas bancarias.	Sí existen otras modalidades, tales como la Suplantación de identidad, sucede cuando estos ciberdelincuentes tienen acceso a la información personal de su víctima y una vez obtenida, pueden hacerse pasar por la persona a quien ha robado los datos.
7	Huaytalla Pillaca Guisella	El fraude informático, que por lo general se asocia con la alteración de datos, ahora es posible vincularla a otros delitos conexos, como es el delito de hurto, al apropiarse de dinero a través de sistemas informáticos, el sabotaje informático, podría considerarse otro modo	En su mayoría, los daños son patrimoniales, entendiendo a los datos informáticos como un bien, que posteriormente permitirá la afectación de otros bienes, como la sustracción de dinero, manipulación de cuentas bancarias, alteración de datos o diseños gráficos de valor económico.	Como otras modalidades podría considerarse al sabotaje, espionaje, incluso tenerse en cuenta el hurto informático, entre otros.

		asociado a la destrucción de los datos.		
8	Guerra Soto Cristhian Miguel	Los más comunes son el phishing y el pharming asociado con la ejecución de operaciones bancarias, ambos entendido dentro de los fraudes informáticos	El fraude informático recae en la provocación de un daño patrimonial a través de la manipulación o alteración de datos o programas de sistemas informáticos, en algunos casos me atrevería a decir daño moral, dado que muchos de los casos no llegan a ser resueltos siendo archivados.	Defraudación, sabotaje, entre otros, habiendo aún más por analizar
9	Lucio Alfredo Zambrano Rodriguez	Por lo general se asocia con la alteración de datos, ahora es posible vincularla a otros delitos por medio de este que posteriormente posibilitara la comisión de otros tipos de delitos.	Principalmente, el daño es de tipo material, por cuanto el bien jurídico afectado es la base de datos e información, entendiendo que esta permite el desenvolvimiento en cuanto al uso de otro medio o plataforma informático.	Desconozco otras tipos de modalidades, pero podría considerarse al sabotaje, espionaje, hurto informático.

10	Hinostroza Rodríguez Carlos	Interferencia telefónica, el fraude informático, entre otros.	Estafa, donde media la sustracción y uso de datos, con consecuencia a la sustracción o apropiación final de dinero, relacionado al daño material en perjuicio del patrimonio, incluso podríamos pensar en un tipo de daño emocional, por cuanto mucho de las denuncias no llegan a formalizarse por falta de ciertos factores, relacionados a pruebas periciales, captación de agente activo, o en cause del tipo penal.	Sabotaje, espionaje, fraude según sus modalidades asociadas a afectación posterior de otros bienes, entre otros.

VALIDACIÓN DE INSTRUMENTO

I.- Datos Generales

1.1Apellidos y nombres: Prieto Chávez Rosas Job
1.2Cargo e Institución donde labora: Docente de la UCV-Ate
1.3Grado Académico: Doctor
1.4Nombre del instrumento de evaluación: Guía de entrevista
1.5Autor del instrumento: Camacho Llantoy, Juan Jips y Figueroa Gonzales, Jhon Bernie

II.- Aspecto de Validación

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Esta formulado con lenguaje comprensible												X	
OBJETIVO	Esta adecuado a las leyes y principios científicos												X	
ACTUALIDAD	Esta adecuada a los objetivos y las necesidades reales de la investigación												X	
ORGANIZACIÓN	Existe una organización lógica												X	
SUFICIENCIA	Toma en cuenta los aspectos metodológico esenciales											X		
INTENCIONALIDAD	Esta adecuado para valorar el desarrollo teórico de la investigación											X		
CONSISTENCIA	Se respalda en fundamentos técnicos y científicos												X	
COHERENCIA	Existe coherencia entre los problemas, objetivos y supuestos jurídicos												X	
METODOLOGIA	La estrategia responde una metodología y diseños aplicados para lograr los supuestos jurídicos												X	
PERTENENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método científico												X	

III.- Opinión de Aplicabilidad

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

si
--

IV.- Promedio de Valoración x **94%**

Lima, 20 mayo de 2022

FIRMA DEL EXPERTO INFORMANTE

DNI N°416513998: Telf.: 922011064

DNI N°416513998: Telf.: 922011064

ANEXO 2

VALIDACIÓN DE INSTRUMENTO

I. **DATOS GENERALES**

1.1. Apellidos y Nombres: Montesinos Córdova, Clemins

1.2. Cargo e institución donde labora: Corte Superior de Justicia Huánuco – Juez

1.3. Nombre del instrumento motivo de evaluación: Guía de entrevista.

1.4. Autor(A) de Instrumento: Camacho Montoy, Juan Sipa y Figueroa Gonzales, Jhon

II. **ASPECTOS DE VALIDACIÓN**

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Está adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Está adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.											X		
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												X	
7. CONSISTENCIA	*Se respalda en fundamentos técnicos y/o científicos.*												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos											X		
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.											X		
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. **OPINIÓN DE APLICABILIDAD**

- El Instrumento cumple con los Requisitos para su aplicación
- El Instrumento no cumple con Los requisitos para su aplicación

SI %
%

IV. **PROMEDIO DE VALORACIÓN:**

95 %

Lima, (fecha).

FIRMA DEL EXPERTO INFORMANTE

CORTE SUPERIOR DE JUSTICIA HUÁNUCO

CLEMINS MONTESINOS CORDOVA
JUEZ

ANEXO 2

VALIDACIÓN DE INSTRUMENTO

I. **DATOS GENERALES**

1.1. Apellidos y Nombres: Balcazar Chilcho, Jaime Alejandro

1.2. Cargo e institución donde labora: Abogado Litigante

1.3. Nombre del instrumento motivo de evaluación: Guía de entrevista.

1.4. Autor(A) de Instrumento: Camacho Llantoy Juan. y Figueroa Gonzales, Jhon

II. **ASPECTOS DE VALIDACIÓN**

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Está formulado con lenguaje comprensible.											X		
2. OBJETIVIDAD	Está adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Está adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.													X
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.													X
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.													X

III. **OPINIÓN DE APLICABILIDAD**

- El Instrumento cumple con los Requisitos para su aplicación
- El Instrumento no cumple con Los requisitos para su aplicación

SI %
%

IV. **PROMEDIO DE VALORACIÓN:**

95 %

Lima, (fecha).
27 de Junio 2022

FIRMA DEL EXPERTO INFORMANTE

Jaime Alejandro Balcazar Chilcho
ABOGADO PENALISTA
CAL 49184

MATRIZ

ANÁLISIS DEL ARTÍCULO 8º DE LA LEY N.º 30171 DE LOS DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO EN EL PERÚ

CATEGORIA:

CATEGORÍAS Y SUBCATEGORÍAS	PROBLEMA	OBJETIVOS	SUPUESTOS	METODOLOGÍA
Categorías 1. Delitos informáticos 2. Patrimonio	**1, Problema General** ¿Cuál es la acción del Estado para afrontar los delitos informáticos contra el patrimonio?	**1.Objetivo General** Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio	a) la acción del Estado para afrontar los delitos informáticos contra el patrimonio es poco eficiente	Método inductivo investigación es de Enfoque cualitativo Tipo Básico Diseño de la investigación Interpretativo
Subcategorías 1.1. Uso de la tecnología en los delitos informáticos 1.2. Perjuicio (daño) de los delitos informáticos 2.1 Modalidades de delitos informáticos contra el patrimonio 2.2 Otros modos de afectación de delitos informáticos contra el patrimonio	**2. Problemas Específicos.** a) ¿Cuál es el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades? b) ¿Cuál es el tratamiento normativo de los Delitos informáticos contra el patrimonio en la modalidad de fraude?	**2. Objetivos Específicos** a) Analizar la eficacia del ordenamiento jurídica de los delitos informáticos contra el patrimonio b) Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades.	**Supuestos Específicos** a) El artículo 8º de la ley N.º 30171 carece de eficacia frente a los delitos informáticos contra el patrimonio b) El tratamiento normativo en cuanto a las modalidades no se encuentra especificadas como tal en los Delitos informáticos contra el patrimonio	

	c) ¿Cuál es el tratamiento normativo de los Delitos informáticos contra el patrimonio en la modalidad de sabotaje? d) ¿Cuál es el tratamiento normativo de los Delitos informáticos contra el patrimonio en la modalidad de estafa?			

FICHA DE ENTREVISTA

Título "Análisis del Artículo 8º **de** la Ley N.º 30171 de los Delitos Informáticos contra el Patrimonio en el Perú"

Entrevistado:

Cargo:

Profesión:

Grado Académico:

Institución:

Objetivos Generales
Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

……
……

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿por qué?

……
……

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

……
……

OBJETIVO ESPECÍFICO 1
Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio

1.- Según su experiencia laboral, ¿considera que el artículo 8º de la ley n.º 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

……

……

……

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

……
……

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

……
……

OBJETIVO ESPECÍFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernéticos?

……
……
……

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

……
……

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

……

……

FICHA DE ENTREVISTA

Título "Análisis del Artículo 8° de la Ley N.° 30171 de los Delitos Informáticos contra el Patrimonio en el Perú"

Entrevistado: Balcázar Chilco, Jaime Alejandro

Profesión: Abogado

Grado Académico: Licenciado especialista en Derecho Penal

Institución: Grupo Themis Abogados SAC.

Objetivos Generales

Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

El Estado debe usar tecnología de última generación a efectos de prevenir y sancionar las conductas ilícitas que afectan a los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿por qué?

Si influyó, porque en los últimos tiempos, se usa las transferencias de dinero, compras, ventas de producto, todo ello virtualmente, entonces la delincuencia se ha especializado a efectos de delinquir, robar y estafar, usando la identidad de las víctimas a efectos de apoderarse de su patrimonio.

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

No está establecido claramente, en todo caso es necesario una mejor y clara tipificación de los delitos informáticos, toda vez que a raíz de la pandemia se han incrementado este tipo de delitos.

OBJETIVO ESPECIFICO 1

Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio

1.- Según su experiencia laboral, ¿considera que el artículo 8º de la ley n.º 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

No esta regulado claramente, porque no se precisa el patrimonio privado, solamente se habla del patrimonio del estado de fines asistenciales.

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

Corresponde al Congreso de la República, legislar al respecto, o caso contrario los fiscales, y jueces informar a efectos de hacer Acuerdos Plenarios al respecto.

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

Doctrina, la Jurisprudencia, Los Acuerdos P´lenarios

OBJETIVO ESPECIFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernéticos?

Por intermedio de Hacker entran a la cuenta y se hacen pasar por la persona dueña de las cuentas, a efectos de apropiarse de dinero, haciéndose transferencias de dinero.

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

Apropiación del dinero de las cuentas

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

Si hay modalidades que tienen que ser incluidos, y sancionados en el código penal.

Jaime Alejandro Balcázar Chilcho
ABOGADO
CAL 49184

FICHA DE ENTREVISTA

Título "Análisis del Artículo 8° de la Ley N.° 30171 de los Delitos Informáticos contra el Patrimonio en el Perú"

Entrevistado: Coaguila Tapia, Percy Leonardo

Profesión: Abogado

Grado Académico: Licenciado especialista en Derecho Penal

Institución: Grupo Themis Abogados SAC.

Objetivos Generales

Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

El estado debería accionar una serie de controles necesarios para resguardar la información cibernética e ir combatiendo estos delitos mediante la firme aplicación de todas las leyes que castigan a quienes los cometen.

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿por qué?

Si, porque el uso de la informática a nivel mundial tiene una importancia relevante frente a la sociedad sobre todo para comunicarse, informarse y realizar movimientos económicos, y esto si influye en el incremento de estos delitos, permitiendo delinquir a los delincuentes.

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

No son reguladas acorde a nuestra realidad. Las medidas se confinamiento y el teletrabajo nos hacen ser más vulnerables a este tipo de delitos y el estado no está tomando en cuenta estos cambios tecnológicos en sus normas.

OBJETIVO ESPECIFICO 1

Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio

1.- Según su experiencia laboral, ¿considera que el artículo 8° de la ley n.° 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

Esta ley no está regulada de manera eficiente, puesto que, con el transcurso de los días, el mundo ha sufrido cambios tecnológicos que dieron inicio e incremento para aquellos sujetos activos quienes aprovechan la tecnología para beneficiarse ilegítimamente del patrimonio de terceros.

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

Para corregir las lagunas o vacíos legales, se debería dar iniciativa legislativa, así tener modificaciones que permitan aplicar las normas de manera eficiente para cada caso en concreto.

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

La fuente principal de nuestro ordenamiento jurídico es la Ley, adecuada al comportamiento humano, sin embargo, es muy necesario que se realice cambios en su contenido, debido a la varianza de nuestra sociedad, y el uso masivo de la tecnología.

OBJETIVO ESPECIFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernéticos?

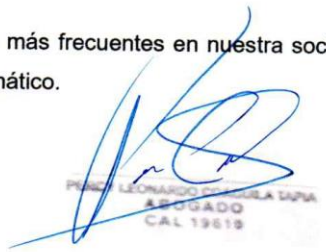
Fraude por la manipulación de computadoras contra un sistema de procesamiento, robo de software y sabotaje informático.

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

He defendido casos de sabotaje informático y robo de servicios.

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

Sí, entre las más frecuentes en nuestra sociedad son los robos de servicios y fraude informático.



FICHA DE ENTREVISTA

Titulo "Analisis del articulo 8° de la ley n.° 30171 de los delitos informáticos contra el patrimonio en el Perú"

Entrevistado: Clenin Montesinos Córdova

Cargo: Juez

Profesión: Abogado

Grado Académico: Bachiller

Institución: Segundo Juzgado de Paz Letrado de Leoncio Prado – Corte Superior de Justicia de Huanuco

Objetivos Generales

Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

El Estado debería afrontar los delitos informáticos a través de una regulación eficaz de nuestra normativa penal, ello a través de un nuevo estudio y análisis correspondiente a través de los organismos y entidades pertinentes dado el incremento de los comportamientos ilícitos constantes que sufren las personas particulares y el Estado.

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿por qué?

Si, principalmente porque los agentes activos valiéndose de sus conocimientos de la informática tienden a perjudicar a las víctimas para beneficiarse ilícitamente de sus bienes patrimoniales.

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

No, en tanto que los cambios tecnológicos en la informática son constantes máxime después del factor COVID-19, en la que en todo ámbito (familiar,

CLENIN MONTESINOS CÓRDOVA
JUEZ
Segundo Juzgado de Paz Letrado - Leoncio Prado

social, etc.) y sector (público, privado) se vale de la informática para el desarrollo de toda actividad y sobre la cual en forma constante se producen comportamientos virtuales ilícitos por parte de los agentes activos que no se encuentran reguladas en la Ley 30171 que fue publicada en el Diario Oficial "El Peruano" el 10 de marzo del 2014.

OBJETIVO ESPECIFICO 1

Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio

1.- Según su experiencia laboral, ¿considera que el artículo 8° de la ley n.° 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

No está regulada de manera suficiente al haber devenido en el tiempo nuevos cambios tecnológicos en la informática que precisamente han dado pies a los agentes tecnológicos quienes en estos últimos tiempos se aprovechan de la virtualidad para beneficiarse en forma deliberada e ilegítimamente del patrimonio de los particulares y del Estado.

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

A través de la modificación o derogación de nuestra normativa legal vigente, según corresponda.

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

Al ser herederos del Sistema Romano-Germánico, considero que la fuente principal para nuestro sistema jurídico penal es la Ley, sobre la cual debe regirse el comportamiento humano de los agentes activos de esta clase de ilirios penales, sin perjuicio de que las mismas sean interpretadas valiéndose de las otras fuentes del derecho.

OBJETIVO ESPECIFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernéticos?

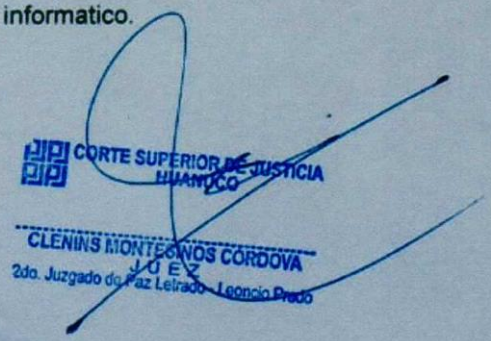
Atentado a los datos informáticos, interferencia telefónica, el fraude informático, entre otros.

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

No he resuelto.

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

Si, las mismas que podrían comprenderse dentro del ilícito penal de fraude informatico.



FICHA DE ENTREVISTA

Título "Análisis del Artículo 8º de la Ley N.º 30171 de los Delitos Informáticos contra el Patrimonio en el Perú"

Entrevistado: Tohalino Aleman, Víctor Manuel

Cargo: Juez Superior

Profesión: Abogado

Institución: Corte Superior de Justicia Lima Este

Objetivos Generales
Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

En nuestro país nos encontramos con que el ordenamiento jurídico en materia penal. No ha avanzado en estos últimos tiempos a diferencia de otras legislaciones, por tanto, es necesario para enfrentar a la llamada criminalidad informática que los tipos peales tradicionales sean revisados, sean actualizados para así consolidar la seguridad jurídica.

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿por qué?

Por supuesto, el avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, han surgido una serie de comportamiento delictivos antes impensables y en algunos casos de difícil tipificación en las normas penales tradicionales.

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

No, efectivamente el desarrollo y masificación de las nuevas tecnologías de la información han dado lugar a cuestiones tales como análisis de la suficiencia del sistema jurídico actual para regular las nuevas posiciones, los nuevos

escenarios, en donde se debaten los problemas del uso y abuso de la actividad informática y su repercusión en nuestra realidad actual.

OBJETIVO ESPECIFICO 1

Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio

1.- Según su experiencia laboral, ¿considera que el artículo 8º de la ley n.º 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

No, la Ley 30096 tenía algunos vacíos, los cuales fueron modificados con la Ley 30171, sin embargo, como nuestra sociedad es cambiante, es necesario realizar modificaciones acordes a los delitos informáticos que se vienen cometiendo.

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

Al tener vacíos, se debe integrar el derecho, esto es, analizar el Derecho como un todo, verlo en su totalidad para buscar una solución ante la ausencia o insuficiencia de regulación para un supuesto específico.

VICTOR M. TOHALINO ALEMAN
JUEZ SUPERIOR
CAL 15418

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

Doctrinas y Jurisprudencias.

OBJETIVO ESPECIFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernético

Las Modalidades más comunes son: el hurto, robo, estafa y defraudaciones.

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

Estafa y defraudaciones

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

Sí existen, y entre ellos debería ser visto con mayor protección el delito de INTRUSISMO.

Victor M. Tohalino Alcanan
JUEZ SUPERIOR
CAL 14418

FICHA DE ENTREVISTA

Titulo "Analisis del artículo 8° de la ley n.° 30171 de los delitos informáticos contra el patrimonio en el Perú"

Entrevistado: Vizcarra Pacheco, Edgar

Cargo: Juez superior

Profesión: Abogado

Institución: Corte Superior de Justicia de Lima Este

Objetivos Generales
Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

Es obligación del estado hacer frente a estos delitos que tienen un aumento significativo en estos tiempos de pandemia, por ello se debe tener una regulación eficaz en nuestra normativa penal, para poder disminuir y hacer frente las conductas antijurídicas de estos cibercriminales.

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿por qué?

Si, porque la falta de educación sobre las amenazas informáticas, concientización, la poca alfabetización digital y la tendencia innata del ser humano a confiar, permitió que los atacantes se aprovechen y vulneren sus patrimonios.

Edgar Vizcarra Pacheco
JUEZ SUPERIOR
CAL [illegible]

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

No, A pesar de los cambios de nuestra sociedad, según el reporte de Ciberseguridad 2020 del BID y la OEA- Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe, El Perú aún no cuenta con una estrategia nacional de seguridad cibernética.

OBJETIVO ESPECIFICO 1

Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio

1.- Según su experiencia laboral, ¿considera que el artículo 8° de la ley n.° 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

No, la Ley 30171, tiene algunos vacíos que deben ser subsanados los más pronto posible, los ciberdelincuentes muchas veces no pueden ser sancionados debido a éstas.

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

Para subsanar estos vacíos es menester del estado, realizar modificaciones y derogar algunas normativas vigentes.

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

Principalmente se acude a las Doctrinas y Jurisprudencias.

Edgar Vizcarra Pacheco
JUEZ SUPERIOR
CAL. 8870

OBJETIVO ESPECIFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernético

Los delitos informáticos que tienen mayor relevancia son los daños o modificaciones de programas o bases de datos, sabotajes, virus o gusanos. En este sentido el solo hecho de hackear el ordenador de una persona se considera un delito.

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

Fraudes, cometidos mediante la manipulación de equipos informático y Falsificaciones informáticas.

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

Si existen otras modalidades, y entre ellas, la que debería ser incluida es la Piratería Informática, el cual son los llamados CRAKERS.

Edgar Vizcarra Pacheco
JUEZ SUPERIOR
CAL 8008

FICHA DE ENTREVISTA

Título "Análisis del Artículo 8º de la Ley N.º 30171 de los Delitos Informáticos contra el Patrimonio en el Perú"

Entrevistado: Huaytalla Pillaca Guissella Rosario

Cargo: Magistrada del tercer juzgado de investigación preparatorio

Profesión: Abogada.

Grado Académico: Superior.

Institución: Poder Judicial del Callao.

Objetivos Generales
Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

Con la llegada de la COVID 19 y el avance tecnológico, el mundo ha dado un cambio de 360 grados, por ello el Estado en interacción de sus distintos órganos jurisdiccionales, deberían someter a mesa estudio, revisar y analizar en busca de posibles deficiencias de la norma, en cuanto a su estructura sustantiva y procedimental, teniendo en cuenta que muchos de los procedimientos penales se dificultan en cuanto a la investigación y enjuiciamiento ya sea; por desconocimiento de los agentes para tratar y obtener prueba digitales, escasez de logística pericial, o dificultad para identificar al autor del delito.

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿Por qué?

Claramente si, influye de forma directa, partiendo de que la tecnología avanza constantemente, siendo un conjunto de conocimientos técnicos, que permite crear, modificar y así adaptar nuestro entorno facilitando las actividades del

hombre, siendo prescindible la presencia física de esta manera siendo el medio y camuflaje que utilizan los sujetos activos, para no ser descubiertos.

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

A pesar de que nuestra legislación respecto a los delitos informáticos, tuvo una reforma en el año 2014 mediante la ley 30171, sería importante evaluar ciertas actualizaciones, en cuanto nuevos posibles tipos penales considerando estos 3 últimos años con la llegada de la COVID 19 y el confinamiento social, la Sociedad tuvo que adaptarse al uso de la tecnología, sin conocimiento adecuado, entre errores, siendo así vulnerables, facilitando la comisión de los delitos informáticos contra el patrimonio, que avanzan a pasos agigantados, valiéndose de nuevas formas y mecanismos para burlar a las autoridades y las normas, e incluso con la implementación de la nueva Fiscalía Corporativa Especializada en Ciberdelincuencia 2021, que es positivo, aun abría más que implementar.

OBJETIVO ESPECIFICO 1

Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio

1.- Según su experiencia laboral, ¿considera que el artículo 8º de la ley n.º 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

La actual legislación artículo 8º de la Ley n.º 30171, carece de eficacia, en cuanto a la falta de expresión talvez de modalidades delictivas que constantemente innovan, anteriormente en el Código Penal artículo 186 inc.4 inciso derogado, refería al uso tecnología, transferencia electrónica como un agravante, creo yo que hoy en día debería tratarse los delitos informáticos en cuanto a sus modalidades teniendo en cuenta al hurto informático, sabotaje, estafa y otros.

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

Partiendo de un estudio y análisis minucioso de la norma regulada desde lo específico hacia lo genérico acorde a nuestra realidad social, mediante la iniciativa del Estado con la intervención de especialistas en el tema, tanto del derecho, como especialistas de las ciencias tecnológicas ya que es necesario comprender la complejidad y funcionabilidad de aquel ciber espacio realidad donde se cometen específicamente estos tipos de delitos.

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

Debido a estas nuevas formas de delinquir basadas en conjeturas, poco familiarizadas o conocidas e en el entorno del derecho, basado en ello otras fuentes a recurrir seria la doctrina, jurisprudencia. Leyes internacionales.

OBJETIVO ESPECIFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernéticos?

El fraude informático, que por lo general se asocia con la alteración de datos, ahora es posible vincularla a otros delitos conexos, como es el delito de hurto, al apropiarse de dinero a través de sistemas informáticos, el sabotaje informático, podría considerarse otro modo asociado a la destrucción de los datos.

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

En su mayoría, los daños son patrimoniales, entendiendo a los datos informáticos como un bien, que posteriormente permitirá la afectación de otros bienes, como la sustracción de dinero, manipulación de cuentas bancarias, alteración de datos o diseños gráficos de valor económico.

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

Como otras modalidades, podría considerarse al sabotaje, espionaje, incluso tenerse en cuenta el hurto informático, entre otros.

FICHA DE ENTREVISTA

Título "Análisis del Artículo 8° de la Ley N.° 30171 de los Delitos Informáticos contra el Patrimonio en el Perú"

Entrevistado: Hinostroza Rodríguez Carlos Francisco.

Profesión: Abogado.

Grado Académico: Magister.

Institución: P.J.

Objetivos Generales
Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

El Estado conjuntamente con sus distintos entes jurisdiccionales están obligados a tomar iniciativa frente a este nuevo tipo de delitos, como son los informáticos, como toda norma que no alcanza la eficacia jurídica que se busca, esta tiene que ser sometida a un profundo análisis, ante los entes especializados, incluso recurrir a profesionales asociados al estudio de software que permitan comprender esta interacción, frente a esta nueva realidad tecnológica.

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿Por qué?

Si influye, la tecnología se ha vuelto indispensable con el pasar de los tiempos para las actividades de la sociedad, pues es este conocimiento de la informática que muy pocos conocemos y es de esta que se valen los agentes activos para la comisión de los distintos delitos informáticos y nuevos tipos criminógenos que hoy en día acontecen.

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

Considero que no son acordes. el desarrollo y extensión de las nuevas tecnologías de la información, han dado lugar a cuestiones tales como análisis en cuanto si es suficiente el sistema jurídico actual para regular las nuevas posiciones, los nuevos escenarios, y tipos delictivos.

OBJETIVO ESPECIFICO 1

Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio.

1.- Según su experiencia laboral, ¿considera que el artículo 8º de la ley n.º 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

No está regulada de manera eficiente, puesto que, con el transcurrir de los días, las sociedades han sufrido cambios tecnológicos, avances, que permitieron la creación de nuevos tipos delictivos asociados a la cibernética.

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

Para corregir los vacíos legales, primero dar iniciativa legislativa, en cuanto revisión y posibles modificaciones de la ley, que permitan aplicar las normas de manera eficiente.

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

Doctrina y jurisprudencia.

OBJETIVO ESPECIFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades.

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernéticos?

Interferencia telefónica, el fraude informático, entre otros.

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

Estafa; donde media la sustracción y uso de datos, con consecuencia a la sustracción o apropiación final de dinero, relacionado al daño material en perjuicio del patrimonio, incluso podríamos pensar en un tipo de daño emocional, por cuanto mucho de las denuncias no llegan a formalizarse por falta de ciertos factores, relacionados a pruebas periciales, captación de agente activo, o en cause del tipo penal.

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

Sabotaje, espionaje, según sus modalidades asociadas a afectación posterior de otros bienes, entre otros.

FICHA DE ENTREVISTA

Título "Análisis del Artículo 8º de la Ley N.º 30171 de los Delitos Informáticos contra el Patrimonio en el Perú"

Entrevistado: Guerra Soto Cristhian Miguel

Cargo: Fiscal Adjunto.

Profesión: Abogado.

Grado Académico: Magister.

Institución: Tercera Fiscalía Corporativa de San Juan de Lurigancho.

Objetivos Generales
Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

He podido reconocer ciertos quiebres sobre los cuales el Estado debería actuar, uno de ellos es la falta de conocimiento y capacitación, tanto de magistrados, fiscales, peritos, abogados y personal policial, entre otros. Segundo la falta de coordinación y comunicación, para trabajar en conjunto, no tan solo entre personal asociados al derecho sino la interacción con especialistas ya sean técnicos, ingenieros, especialistas en software.

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿Por qué?

Si influye, la tecnología hoy en día implica una necesidad para la vida del hombre, el avance de esta sin tener de tras un medio adecuado de contingencias para supervisar a quienes lo usan, lo ha convertido en un factor criminógeno que posibilita la vulneración de derechos a la privacidad e intimidad mediante el acceso a nuestras plataformas electrónicas privadas y así manipular y

apropiarse de datos de información pudiendo estos tener valor económico como cuentas bancarias , proyectos, etc. y así afectar el patrimonio.

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

En realidad, no son acordes, a mi parecer, la descripción de la norma asociada a los delitos informáticos contra el patrimonio es genérica con falta de especificaciones en cuanto al patrimonio privado entendido como un supuesto y falta especificar respecto a las formas.

OBJETIVO ESPECIFICO 1

Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio.

1.- Según su experiencia laboral, ¿considera que el artículo 8º de la ley n.º 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

Para alcanzar la eficacia, a mi parecer faltaría un análisis profundo de la norma para una adecuada redacción de los delitos informáticos contra el patrimonio, relacionados al artículo 8 de fraudes, considerando las conductas que normalmente se califican como tales, podrá constatarse que el término fraude informático es entendido de forma bastante más amplia y que, en ese sentido, suelen incluirse comportamientos muy diversos.

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

Ello recae en los legisladores, ejecutivo y magistrados mediante el interés e iniciativa de poder poner en observación y análisis la norma asociada para así poder subsanar las falencias que se encuentren, e incluso tomar en cuenta las aportaciones o críticas constructivas de los distintos agentes asociados a estos casos, de delitos informáticos.

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

Doctrina, jurisprudencia y Leyes internacionales

OBJETIVO ESPECIFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades.

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernéticos?

Los más comunes son el phishing y el pharming asociado con la ejecución de operaciones bancarias, ambos entendido dentro de los fraudes informáticos

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

El fraude informático recae en la provocación de un daño patrimonial a través de la manipulación o alteración de datos o programas de sistemas informáticos, en algunos casos me atrevería a decir daño moral, dado que muchos de los casos no llegan a ser resueltos siendo archivados.

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

Defraudación, sabotaje, entre otros, quedando aún más por analizar.

Cristhian Miguel Guerra Soto
Fiscal Adjunto Provincial
1° Fiscalía Provincial Penal Corporativa
de S.J.L. - Zona Media - 3° Despacho

FICHA DE ENTREVISTA

Título "Análisis del Artículo 8° de la Ley N.° 30171 de los Delitos Informáticos contra el Patrimonio en el Perú"

Entrevistado: Lucio Alfredo Zambrano Rodriguez

Cargo: Notario

Profesión: Abogado

Grado Académico: Superior

Institución: Universidad San Martín de Porres

Objetivos Generales

Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

El Estado debería actuar en 2 aspectos, uno de ellos es la falta de conocimiento y capacitación, tanto de magistrados, fiscales, peritos, entre otros. Segundo, la falta de coordinación entre estos agentes que son pieza fundamental en el proced.

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿por qué?

Si influyó, la tecnología hoy implica una necesidad para la vida del hombre, el avance de ésta sin tener detrás un medio adecuado de contingencias para supervisar a quienes lo usan, convertio en un factor criminógeno que posibilita la vulneración de derechos a la privacidad e intimidad.

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

No son acordes a mi parecer, la descripción de la norma asociada a los delitos informáticos contra el patrimonio es genérica. con falta de especificaciones.

OBJETIVO ESPECIFICO 1

Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio

1.- Según su experiencia laboral, ¿considera que el artículo 8° de la ley n.° 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

Carece de eficacia en cuanto a la falta de expresión de las modalidades delictivas que constantemente innovan con el pasar del tiempo.

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

Partiendo de un estudio y analisis minucioso de la norma regulada desde lo específico hacia lo genérico acorde a nuestra realidad social, mediante la iniciativa del Estado con la intervención de especialistas en el tema.

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

Doctrinas y Jurisprudencias.

OBJETIVO ESPECIFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernéticos?

Por lo general se asocia con la alteración de Datos, ahora es posible vincularla a otros delitos por medio de este, que posteriormente posibilitará la comisión de otros tipos de delitos.

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

Principalmente el daño es de tipo material, por cuanto el bien jurídico afectado es la base de datos y la información, entendiendo que ésta permite el desenvolvimiento en cuanto al uso de otro medio o plataforma informático.

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

Desconozco otra tipo de modalidades; pero se podría considerar al sabotaje, espionaje, hurto informático

Alfredo Zambrano Rodriguez
NOTARIO DE LIMA

FICHA DE ENTREVISTA

Título "Análisis del Artículo 8° de la Ley N.° 30171 de los Delitos Informáticos contra el Patrimonio en el Perú"

Entrevistado: Cerón Salazar, Nelson
Cargo: Abogado Litigante
Profesión: Abogado
Grado Académico: Superior
Institución: Universidad Inca Garcilaso de la Vega

Objetivos Generales

Analizar la intervención del Estado para afrontar los delitos informáticos contra el patrimonio

1.- ¿Según su experiencia, de qué manera el Estado debería afrontar los delitos informáticos?

El Estado debería promover convenios multilaterales que ayuden a disminuir los delitos informáticos, con ello tener cooperación mutua con otros Estados. Los ciberdelincuentes están un paso adelante, saben los deficiencias y antigüedades, por ello la importancia de la cooperación con los otros Estados.

2.- ¿Considera usted que el uso de la tecnología, influyó en el incremento de los delitos contra el patrimonio? ¿por qué?

Por supuesto que sí, y no solo en nuestro país, incluso en países con tasas de inseguridad muy bajas, el uso de la Tecnología se ha convertido en uno de los principales factores que ayudaron al incremento de los delitos informáticos contra el patrimonio

3.- Según su percepción, ¿Considera que las leyes respecto a los delitos informáticos contra el patrimonio son reguladas acorde a nuestra realidad actual 2021?

Nuestras leyes sí están reguladas acorde a nuestra realidad social, el problema se encuentra en la interpretación de estas leyes por parte de algunos colegas, quienes por falta de capacitaciones en la cuestión informática, no aplican de manera adecuada la Ley. 30171, ha citada norma incorporó delitos tales como: interceptación de información, suplantación de identidad, entre otros, a si mismo se les estableció sanciones penales para contrarrestar su consumación, por ello ya depende de los operadores de Justicia.

OBJETIVO ESPECIFICO 1

Analizar la eficacia del ordenamiento jurídico de los delitos informáticos contra el patrimonio

1.- Según su experiencia laboral, ¿considera que el artículo 8° de la ley n.° 30171 de los delitos informáticos contra el patrimonio, está regulado de manera suficiente para garantizar su eficacia?

Sí, ya antes lo había mencionado, si bien es cierto la ley 30096 tenía algunos vacíos éstas fueron modificadas por la ley 30171, ley que cumple a cabalidad para garantizar los delitos que vulneren el artículo 8°, sobre los delitos informáticos contra el patrimonio....

2.- ¿Cómo se podría corregir los vacíos legales de nuestra normativa con respectos a los delitos informáticos contra el patrimonio?

Desde una perspectiva objetiva, la ley 30096 sí tenía algunos vacíos, y que fueron... subsanados con la ley 30171, ley que sí garantiza los delitos que vulneren... el artículo 8°, sobre los delitos informáticos contra el patrimonio.....

3.- ¿Cuál es la otra fuente del derecho aplicada para remediar los vacíos legales respecto a los delitos informáticos contra el patrimonio?

Ante la existencia de vacíos, existen algunas fuentes aplicables al derecho, tenemos los tratados internacionales, constituciones, leyes, reglamentos, así mismo están las doctrinas, la costumbre, y los principios generales al derecho consagrados... por la jurisprudencia.

OBJETIVO ESPECIFICO 2

Analizar el tratamiento normativo de los delitos informáticos contra el patrimonio en sus distintas modalidades

1.- ¿cuáles considera usted que son las modalidades más usuales o comunes cometidos por los delincuentes cibernéticos?

Entre los mas comunes y denunciados son los fraudes informáticos, las estafas virtuales y las suplantaciones de identidad, todos estos forman parte de lo q' denominamos "Ciberdelincuencia", de acuerdo a las estadísticas que me ha tocado defender:...

2.- De acuerdo a los casos que usted ha resuelto, ¿qué tipo de daños son los más frecuentes causados por la comisión de los delitos informáticos contra el patrimonio?

Me ha tocado defender muchos casos de Apropiación Ilícita de..... ..... dinero... de las cuentas bancarias.....
.....

3.- ¿Considera usted que existen otras modalidades de delitos informáticos contra el patrimonio que debería ser incluidos en nuestro ordenamiento jurídico?

Sí existen otras modalidades tales como la Suplantación de Identidad, sucede cuando estos ciberdelincuentes tienen acceso a información personal de su víctima, y una vez obtenida, pueden hacerse pasar por la persona a quien ha robado los datos.

CERON SALAZAR, NELSON
ABOGADO PENALISTA

República de Colombia
Corte Suprema de Justicia
Sala de Casación Penal

CORTE SUPREMA DE JUSTICIA
SALA DE CASACIÓN PENAL
SALA DE DECISIÓN DE TUTELAS N° 1

GUSTAVO ENRIQUE MALO FERNÁNDEZ
Magistrado ponente

STP6279-2017
Radicado N° 91612.
Aprobado acta N° 126.

Bogotá, D.C., cuatro (4) de mayo de dos mil diecisiete (2017).

VISTOS

Decide la Sala, en primera instancia, la acción de tutela promovida por el ciudadano **JUAN FELIPE OCAMPO OSORIO**, para la protección de sus derechos fundamentales al debido proceso, igualdad y defensa, presuntamente

vulnerados por la **Sala Penal del Tribunal Superior del Distrito Judicial de Bogotá** y el **Juzgado 39 Penal del Circuito con Funciones de Conocimiento** de la capital del país, trámite al cual se dispuso la vinculación del **Juzgado 28 Penal Municipal Con Función de Control de Garantías** y la **Fiscalía 115 Seccional**, ambos de la capital del departamento de Cundinamarca, así como a las partes y demás sujetos intervinientes dentro proceso penal que cursó en su contra por los delitos de hurto por medios informáticos agravado en concurso heterogéneo con acceso abusivo a un sistema informático agravado, violación de datos agravado, falsedad en documento privado y concierto para delinquir, radicado con el No. 110016100000020110032.

HECHOS Y FUNDAMENTOS DE LA ACCIÓN

De acuerdo con el escrito de tutela y demás documentos obrantes en el expediente se extrae que, por allanamiento a cargos, mediante sentencia del 28 de septiembre de 2011, el accionante fue condenado por el Juzgado 39 Penal del Circuito con Funciones de Conocimiento de esta urbe a la pena principal de 101 meses de presidio y multa de 105 salarios mínimos legales mensuales vigentes como coautor de los punibles de hurto por medios informáticos agravado, en concurso heterogéneo con acceso abusivo a un sistema informático agravado, violación de datos agravado, falsedad

TRIBUNAL CONSTITUCIONAL

Pleno. Sentencia 1100/2020

EXP. N.° 01189-2019-PHC/TC
LIMA
MARCOS MORALES VARGAS, representado por WILLIAM BENARDINO GARCÍA ROSALES

RAZÓN DE RELATORÍA

En la sesión del Pleno del Tribunal Constitucional de fecha 10 de diciembre de 2020, los magistrados Ledesma Narváez, Ferrero Costa, Miranda Canales, Ramos Núñez, Sardón de Taboada y Espinosa-Saldaña Barrera han emitido, por mayoría, la siguiente sentencia que declara **INFUNDADA** la demanda de *habeas corpus* que dio origen al Expediente 01189-2019-PHC/TC.

Se deja constancia que el magistrado Blume Fortini emitirá su voto en fecha posterior.

La Secretaría del Pleno deja constancia de que la presente razón encabeza la sentencia antes referida, y que los magistrados intervinientes en el Pleno firman digitalmente al pie de esta razón en señal de conformidad.

Flavio Reátegui Apaza
Secretario Relator

SS.

LEDESMA NARVÁEZ
FERRERO COSTA
MIRANDA CANALES
BLUME FORTINI
RAMOS NÚÑEZ
SARDÓN DE TABOADA
ESPINOSA-SALDAÑA BARRERA

EXP. N.° 01189-2019-PHC/TC
LIMA
MARCOS MORALES VARGAS, representado por WILLIAM BENARDINO GARCIA ROSALES

SENTENCIA DEL TRIBUNAL CONSTITUCIONAL

En Lima, a los 10 días del mes de diciembre de 2020, el Pleno del Tribunal Constitucional, integrado por los magistrados Ledesma Narváez, Ferrero Costa, Miranda Canales, Ramos Núñez, Sardón de Taboada y Espinosa-Saldaña Barrera, pronuncia la siguiente sentencia. Se deja constancia de que el magistrado Blume Fortini votará en fecha posterior.

ASUNTO

Recurso de agravio constitucional interpuesto por don William Benardino García Rosales, abogado de don Marcos Morales Vargas, contra la resolución de fojas 421, de fecha 5 de noviembre de 2018, expedida por la Segunda Sala Penal para Procesos con Reos Libre de la Corte Superior de Justicia de Lima, que declaró improcedente la demanda de *hábeas corpus* de autos.

ANTECEDENTES

Con fecha 18 de julio de 2018, don William Benardino García Rosales interpone demanda de *hábeas corpus* a favor de don Marcos Morales Vargas (f. 31) y la dirige contra los jueces integrantes de la Primera Sala Penal de la Corte Superior de Justicia de Lima Norte y la jueza a cargo del Décimo Juzgado Penal de Lima Norte.

Solicita que se declare la nulidad de: (i) la sentencia de 16 de junio de 2017 (f. 3), que condenó al beneficiario por los delitos de fraude informático y falsificación de firma en documento privado; y (ii) la Resolución de 26 de diciembre de 2017 (f. 73), que confirmó la precitada sentencia en cuanto a la condena, pero la revocó respecto a la pena; y, reformándola, le impuso ocho años de pena privativa de la libertad efectiva (Expediente 9405-2014). Se alega la vulneración de los derechos a la libertad personal, al debido proceso y a la tutela jurisdiccional efectiva, así como del principio de legalidad penal.

Sostiene que mediante la sentencia de 16 de junio de 2017, se condenó al beneficiario a diez años de pena privativa de la libertad efectiva, que resultó de la sumatoria siguiente: ocho años por el delito de fraude informático y dos años de pena privativa de la libertad efectiva y falsificación de firma en documento privado. Posteriormente, mediante la Resolución de 26 de diciembre de 2017, se le redujo la pena a seis años de pena privativa de la libertad efectiva, por ambos delitos.

Precisa que se condenó al beneficiario a través de una norma que no se encontraba vigente al momento que se cometieron los hechos delictuosos, pues tales hechos ocurrieron durante los meses de enero, febrero, marzo, julio, setiembre y octubre de 2013, pero fue