FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Carrera de **DERECHO Y CIENCIAS POLÍTICAS**

“EL PROCESAMIENTO PENAL DE LA PERSONA JURÍDICA INVOLUCRADA EN LA COMISIÓN DE DELITOS INFORMÁTICOS EN EL PERÚ, 2022”

Tesis para optar el título profesional de:

ABOGADO

Autor:

Renzo Jesus Vasquez Villacorta

Asesor:

Dr. Noe Valderrama Marquina

https://orcid.org/0000-0002-8696-3179

Lima - Perú

2022

JURADO EVALUADOR

Jurado 1 Presidente(a)	YSAAC MARCELINO ARCOS FLORES	**06976352**
	Nombre y Apellidos	N.º DNI

Jurado 2	Flor De María Madela Poma Valdivieso	**25576850**
	Nombre y Apellidos	N.º DNI

Jurado 3	Harold Velazco Marmolejo	**42390174**
	Nombre y Apellidos	N.º DNI

DEDICATORIA

A mi madre, Maritza, mujer de espíritu inquebrantable a la cual le debo todo.

AGRADECIMIENTO

A mis padres, Tito y Maritza, por todo el trabajo y esfuerzo para hacer esto realidad; a mi hermano Carlos, el primer amigo que tuve y que siempre estará conmigo.

A mis amigos, compañeros, y docentes, con los cuales recorrí este camino lleno de experiencias, emociones y aprendizajes.

A todas las personas que creyeron en mi y me dieron la oportunidad de seguir creciendo profesionalmente.

A Dios, porque aún en la noche más oscura, nunca dejo hacer brillar la luz de una estrella para mí.

Tabla de contenido

JURADO CALIFICADOR 2

DEDICATORIA 3

AGRADECIMIENTO 4

TABLA DE CONTENIDO 5

ÍNDICE DE TABLAS 6

ÍNDICE DE FIGURAS 7

RESUMEN 8

CAPÍTULO I: INTRODUCCIÓN 9

CAPÍTULO II: METODOLOGÍA 48

2.1. Tipo de investigación 48

2.2. Población y muestra 50

CAPÍTULO III: RESULTADOS 60

CAPÍTULO IV: DISCUSIÓN Y CONCLUSIONES 83

4.1. Limitaciones 83

4.2. Discusión 84

4.3. Conclusiones 93

REFERENCIAS 96

ÍNDICE DE TABLAS

1. TABLA 1 50
2. TABLA 2 51
3. TABLA 3 60
4. TABLA 4 65
5. TABLA 5 67
6. TABLA 6 72
7. TABLA 7 76
8. TABLA 8 81

ÍNDICE DE FIGURAS

1. FIGURA 1 89

RESUMEN

En los últimos años el Derecho Penal ha atravesado por un proceso de evolución conforme la sociedad desarrolla nuevas conductas criminógenas y espacios delictivos. En dicho sentido, en Derecho Penal de la Empresa y los Delitos Informáticos o Cibercrímenes representan un reto para la justicia penal convencional, implicando un cambio de enfoque del Derecho Penal clásico, y una reforma procesal y dogmática para hacer frente a estos nuevos fenómenos delictivos. El presente trabajo tiene como objetivo determinar si existe un procesamiento penal adecuado de la persona jurídica involucrada en la comisión de delitos informáticos en el Perú al año 2022, así como analizar los elementos de juicio para incorporarla a un proceso penal por delitos informáticos, y proponer una fórmula adecuada de procesamiento penal para entes colectivos en casos de cibercrímenes. En dicho sentido la presente investigación es de orden cualitativa y exploratoria, al ser el primer estudio sobre la materia, brindando así el soporte dogmático y las bases teóricas para que los operadores de justicia penal puedan tratar adecuadamente los casos relacionados a empresas y delitos informáticos, llegando a la conclusión que los delitos informáticos deben ser incorporados en el catálogo de delitos de la Ley 30424, Ley que Regula la Responsabilidad Administrativa de la Persona Jurídica.

PALABRAS CLAVES: Delitos informáticos, cibercrimen, responsabilidad penal de la persona jurídica, empresas, *compliance*

CAPÍTULO I: INTRODUCCIÓN

1.1. Realidad problemática

En la actualidad es innegable el desarrollo vertiginoso de las tecnologías de la información y comunicación o también denominadas TIC, las mismas que han revolucionado la forma en que los seres humanos se comunican y relacionan, por lo que la sociedad viene adaptándose de forma constante a los avances tecnológicos y a la cada vez más imponente presencia del internet y la vida en el ciberespacio.

De este modo, hemos pasado de la sociedad de las masas del siglo pasado a la denominada sociedad de la información, en la cual los datos y el conocimiento han tomado un papel protagónico en nuestra sociedad, así también este desarrollo va de la mano con una dimensión tecnológica, debido a que la sociedad de la información no puede ser representada sin los elementos técnicos que la hacen posible. De este modo las tecnologías de la información se han transformado en un acompañante fundamental de nuestra sociedad, y son los descubrimientos tecnológicos los que tienen la capacidad transformadora de forma histórica en nuestra sociedad (Crovi, 2005).

Asimismo, cabe resalta la importancia financiera y económica que tiene la información en nuestra sociedad, constituyendo un activo de relevancia significativa para las empresas y corporaciones, así como en los servicios públicos como educación, salud y alimentación (Alfonso, 2016). Estas nuevas estructuras sociales brindan nuevos elementos, y bienes jurídicos a proteger, como la identidad digital y la confidencialidad de la información, siendo que, en ecosistemas virtuales de interconexión de datos, como lo es la

Internet, el concepto de libertar digital cobra un nuevo sentido, junto a las indeterminadas formas de aplicación y desarrollo que tiene como potencial.

De este modo, dicho desarrollo tecnológico, y acompañado por la reestructuración de los fundamentos sociales y sus espacios de relación e interconexión, abren las puertas a un mundo de posibilidades a explotar para el desarrollo actividades económicas, sociales, culturales, comerciales, gubernamentales y otras no determinadas.

Sin embargo, ante la libertad y posibilidades de aplicación indeterminadas que ofrecen las Tecnologías de la Información y Comunicación (TIC's) y la interacción digital, este se convierte en un ambiente propicio para el surgimiento de nuevos fenómenos criminógenos, y la aparición de conductas delictivas virtuales, sea como instrumentalización de las TIC para la comisión de delitos comunes (estafa, extorsión, etc.), o para la comisión de delitos propios de ambientes virtuales o sistemas informáticos (robo de información, acceso no autorizado, etc.).

Así pues, el desarrollo continuo y la proliferación de las tecnologías de la información representan un reto para la justicia penal, siento que se han convertido en un instrumento ideal para la internacionalización del crimen y el favorecimiento de las actividades de organizaciones criminales transnacionales (Reyna, 2016).

En esa misma línea, el desarrollo de las TIC a partir del internet, ha traído diferentes cambios en la interacción humana, como la transmisión de datos y comunicación instantánea, así como el cibergobierno, cibereducación o cibersalud, pero que, si bien, han traído mejoras sustanciales al desarrollo humano, también se deben tener en cuenta los riesgos relacionados al uso de las tecnologías informáticas y de comunicación, dado que

estas traen consigo nuevas formas delictivas que tienen como medio o finalidad los sistemas informáticos e internet (Villavicencio, 2014).

En efecto, los casos de criminalidad informática que involucran entes corporativos son cada vez mayores y con mayor incidencia en el campo internacional, afectando dichas personas jurídicas tanto como sujeto activo o pasivo, sea por ciberataques, o por vulneraciones de seguridad en el propio seno de la persona jurídica.

Tal es el caso, que la consultora internacional Deloitte, en su estudio del 2021 sobre el estado de la ciberseguridad en España, donde concluyó que al menos el 94% de las empresas españolas se han visto inmersas en un incidente grave de ciberseguridad, lo que, en aplicación de un enfoque político-criminal, hace que dichas empresas corran el riesgo de verse involucradas en investigaciones penales por comisión de delitos informáticos. Por otro lado, tenemos el caso de la red cibercriminal ZLoader especializada en robo y extorsión cibernética, la misma que el año presente 2022 hubiera sido desmantelada por la Unidad de Crímenes Digitales de Microsoft. Dicha red utilizaba en base a la técnica de malware como servicio, encriptando información de sus víctimas para luego extorsionarlas pidiendo el pago de un rescate a cambio de devolver la información. Entre los afectados se encuentran empresas, hospitales, escuelas y particulares, víctimas de secuestro de información.

Un caso relevante y particularmente interesante, el de Amazon ante el ente regulador de datos personales de la Unión Europea el 2021, cuando fue sancionada con una multa récord de US$ 887 millones de dólares, ello debido a que el ente regulador europeo consideró que Amazon no cumplía los requisitos de su normativa de protección de datos personales, estipulado en la General Data Protection Regulation (GDPR). Dicha sanción versa sobre un tratamiento inadecuado por parte de Amazon de la información personal de sus usuarios,

que, si bien no tiene índole criminal, ha quedado advertido el riesgo y posibles consecuencias legales, que al no ser abordadas de forma adecuada podría generar implicancias penales.

Por otro lado, otro caso que atrajo especial interés internacional fue el que involucró al gigante tecnológico Facebook y la consultora Cambridge Analytica, en un caso de venta de información personal masiva para fines publicitarios y políticos. Siendo que si bien Facebook no vendió ni utilizó información sensible de sus usuarios, su sistema fue aprovechado por terceros para recolectar información de más de 50 millones de personas, información que luego fue vendida a Cambridge Analytica la cual realizó perfiles psicológicos en base a dicha información, la misma que utilizó para direccionar las acciones de personas dentro de un contexto de elecciones políticas. Si bien es cierto, en el citado caso se advirtió que Facebook no habría realizado acción vulneradora, o vendido los datos personales de sus usuarios, si se aceptó que terceros utilizaron vacíos de seguridad de propia plataforma para obtener datos sensibles, lo cual hizo que Facebook modifique sus condiciones y configuraciones de privacidad, no obstante dicho caso advierte sobre la gran capacidad de almacenamiento y procesamiento de información sensible que poseen grandes empresas de prestación de servicios digitales como Facebook, relacionados en el caso concreto con Big Data y tecnología algorítmica, capaz de influir y conducir la forma de pensar y decisiones de millones de personas.

En referencia al Perú, las empresas peruanas no han sido ajenas la cibercriminalidad, según la consultora Ernst & Young en su Encuesta Global sobre la Seguridad de la Información 2021, arrojaría que 5% de los directores de seguridad de la información manifestaron un aumento en la cantidad de ciberataques disruptivos desde el 2020, y un 63% manifestó gran preocupación por la capacidad de sus empresas para gestionar esta clase de riesgos informáticos. En ese sentido, son las entidades financieras y las prestadoras de

servicios digitales las que presentan una mayor exposición a verse envueltas en delitos informáticos, tal es el caso del Banco de Crédito del Perú – BCP, el cual declaró haber sufrido un robo masivo de datos el 2018, donde se filtraron números de tarjetas y de cuenta de cierto grupo de usuarios.

Los casos expuestos denotan, los riesgos informáticos, especialmente relacionados a personas jurídicas, que por la información sensible que almacenan, así como por su alcance y capacidades tecnológicas, pueden verse envueltas en vulneraciones de ciberseguridad o involucradas en casos de cibercriminalidad, cometida mediante sus funcionarios u operarios, que dependiendo del tipo de vulneración podría escapar de las normas de protección de datos personales para calificarse con un delito informático mediante la instrumentalización de una persona jurídica, a lo cual el derecho penal y procesal penal no puede mantenerse ajeno.

Sociedad de riesgo y globalización

La globalización y las sociedades posindustriales han conectado al mundo como nunca, siendo que el desarrollo de las libertades individuales, como el crecimiento económico de los Estados, ha traído enormes cambios para sociedad, y por ende sobre las legislaciones nacionales e internacionales, las cuales deben evolucionar sus alcances y márgenes de jurisdicción e intervención estatal, de lo contrario serían sobrepasadas deviniendo el Derecho Público en inútil para su regulación. Estos cambios y procesos de interrelación, evolución, e interconexión social se presentan en diversos aspectos de la vida humana, tanto políticos, religiosos, educativos, comerciales, tecnológicos, científicos y económicos. (CEPAL ONU, 2002). Sin embargo, este denominado avance posindustrial ha generado nuevos fenómenos de riesgo global, es decir, por ejemplo, que hasta el siglo XIX

no podría concebirse la idea de países enteros en cuarentena total, o conflictos sociales y económicos que desencadenen en reales efectos dominó a nivel internacional.

Recurriendo a los inicios de estos cambios, la primera y segunda guerra mundial, y el inicio de la era atómica advirtieron al mundo y a los científicos que los peligros que podían enfrentar las sociedades habían alcanzado niveles globales. Es decir, riesgos o peligros que en un pasado podían afectar a comunidades, o pocos países, con el avance de la ciencia, la globalización, la interdependencia económica, y otros factores, afectarían en la actualidad a continentes enteros o a todo el mundo.

Lo anterior fue explicado por primera vez en 1986 por el sociólogo Ulrich Beck, en su obra denominada "La sociedad de riesgo". En la obra citada, el autor también describe lo que denomina el "efecto bumerán", es decir, que los entes generadores del riesgo tarde o temprano se ven afectados por este (Beck, 1986). Este concepto nos es especialmente interesante, ya que, para fines de este trabajo, y a nuestra consideración, uno de los entes generadores de riesgo más importantes -si es que no es el más importante- en mundo posindustrial, no es el Estado, si no el sujeto privado organizado en entes colectivos, de finalidad lucrativa o no lucrativa, es decir las denominadas empresas o corporaciones, que dentro del desarrollo de sus actividades económicas, las cuales son muchas veces a gran escala (gran minería, telecomunicaciones, ciencia aeroespacial, vacunación poblacional, big data, etc.) generan un alto riesgo, donde la ausencia de una cultura de responsabilidad social corporativa o RSE, puede generar graves consecuencias sociales o materiales. En efecto, el enfoque corporativo contemporáneo propugna la generación de empresas socialmente responsable, que más allá de tener solo una finalidad exclusivamente lucrativa, generen un aporte positivo a la sociedad y a la humanidad (CEGESTI, 2016)

La ley de delitos informáticos

Con el auge de la sociedad de la información, los delitos informáticos han cobrado un espacio cada vez más importante en las legislaciones nacionales e internacionales. En dicho sentido, en el 2001 se acordó el Convenio sobre la ciberdelincuencia o Convenio de Budapest, en el cual se acordaron principios dogmáticos y procesales a nivel internacional sobre la lucha contra la ciberdelincuencia y su persecución penal, para que de esta forma poder establecer las bases esenciales que deben optar los países firmantes para legislar sobre estos delitos. Dicho convenio ha sido firmado y ratificado por el Perú, el mismo que entró en vigor en marzo del 2019.

Dentro de la legislación nacional, se encuentra regulada la ley 30096, denominada Ley de Delitos Informáticos, modificada por la ley 30171, constituyéndose como la principal norma contra la cibercriminalidad en el Perú, en reemplazo de los antiguos delitos informáticos establecidos en el Código Penal Peruano y que actualmente se encuentran derogados. Cabe mencionar que dicha norma ha sido criticada por parte de la doctrina, argumentando que no cumple con los objetivos de sancionar adecuadamente los delitos informáticos, si no, que solo se elaboró dicha normativa para cumplir formalmente con las obligaciones del Perú como país firmante del Convenio de Budapest, por lo que a la fecha se ha emitido el Proyecto de Ley 5630/2020-CR Ley de Seguridad Informática y Represión de los Delitos Informáticos, que busca reemplazar la normativa vigente de la materia, no obstante a la fecha dicho proyecto de ley aún no sigue en revisión.

Ahora bien, de acuerdo con el Artículo 1° de la Ley de Delitos Informáticos, dicha norma tiene por finalidad prevenir y sancionar las conductas ilícitas que afecten los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, que sean cometidas

mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

En dicho sentido, la norma tipifica los siguientes delitos:

- Acceso ilícito a sistemas informáticos (Art. 2)
- Atentado contra la integridad de datos informáticos (Art. 3)
- Atentado contra la integridad de sistemas informáticos (Art. 4)
- Proposiciones a niños, niñas u adolescentes con fines sexuales por medios tecnológicos (Art. 5)
- Tráfico ilegal de datos (Art. 6)
- Interceptación de datos informáticos (Art. 7)
- Fraude informático (Art. 8)
- Suplantación de identidad (Art. 9)
- Abuso de mecanismo y sistemas informáticos (Art. 10)

De esta forma la norma tipifica las principales conductas penales cibernéticas, divididos cinco títulos, divididos en a) delitos informáticos contra datos o sistemas informáticos, b) delitos informáticos contra la indemnidad o libertad sexuales, c) delitos informáticos contra el patrimonio, d) delitos informáticos contra la fe pública, y e) como disposición común, el abuso de mecanismos o dispositivos informáticos (desarrollo de malware, virus informático o cualquier tipo de soporte a la criminalidad informática).

Del mismo modo establece técnicas especiales de investigación para delitos informáticos, como el agente encubierto y el levantamiento del secreto de telecomunicaciones, así como diversas disposiciones de índole administrativo que faciliten

la cooperación institucional entre el Ministerio Público y la Policía Nacional para hacer frente a estos delitos.

Adicionalmente, un punto que vale la pena mencionar es que dicha norma carece de un apartado dedicado a personas jurídicas relacionadas o involucradas a la comisión de delitos informáticos, es decir que se encuentra solamente orientada a la persona natural, limitándose solamente a hacer referencia las obligaciones de entrega de información de las empresas proveedoras de servicios de internet.

Expansión del Derecho Penal

Como consecuencia de la gran expansión de riesgos en la sociedad, el Estado debe fortalecer sus mecanismos de control social, los cuales aún con el fortalecimiento de políticas educativas y medidas de control administrativas, pueden verse ampliamente superadas, por lo que, ante la inefectividad de medidas de control menos gravosas, es necesario recurrir al Derecho Penal como forma de control social formal, a fin de resguardar bienes jurídicos protegidos de los particulares y la sociedad. Dicha expansión se da mediante una reformulación de la política criminal y los preceptos sociales de control, reformando barreras de punibilidad que, a fin de buscar mayor protección penal, adecuan diversas conductas humanas, sean económicas o empresariales a tipos penales mediante un recrudecimiento de los marcos punitivos, especialmente en temas del Derecho Penal Económico y medioambiental (Escobar, 2009).

En esa línea, la aparición de nuevos intereses sociales y económicos -aparición de nuevas valoraciones- será vital para la creación de nuevos bienes jurídicos protegidos, legitimados de protección penal, como las instituciones económicas, inversión o propiedad intelectual. Asimismo, la relación de este concepto de expansión penal tiene plena relación

con la obra de Ulrich Beck, sobre la sociedad de riesgo, estableciendo que vivimos en una sociedad altamente cambiante por los marcos económicos, y el avance vertiginoso y cada vez más acelerado de la tecnología como nunca se ha registrado en la historia de la humanidad, y que dichas revoluciones técnicas han traído grandes repercusiones en el bienestar individual (Silva, 2006).

Empresa y Derecho Penal

Como venimos exponiendo, en concordancia con los presupuestos teóricos de la denominada sociedad de riesgo y la expansión del Derecho Penal -aumento de riesgos no permitidos-, una de las entidades que genera un especial riesgo por su actividad es la empresa como ente organizado. En dicho contexto, en la actualidad observamos que la empresa se ha convertido en el principal motor económico y de avance e innovación científica de la sociedad, desarrollándose en todos los campos de la actividad humana.

En efecto, debido a la globalización y la apertura de mercados internacionales, en conjunto con el desarrollo de nuevas tecnologías, ha llevado a las empresas a tener el objetivo de aumentar su crecimiento económico y nivel de influencia. Esta expansión de la empresa como principal motor económico de las sociedades ha llevado a ampliar su gama de posibilidades de forma exponencial (Puerto, 2010).

Dicho desarrollo corporativo ha traído como resultado que existan corporaciones multinacionales con ingentes patrimonios, incluso comparable al PBI de pequeños países, especialmente las compañías relacionadas al desarrollo de tecnología informática, denominados los “gigantes tecnológicos”, tal es el caso de Microsoft, compañía estadounidense valorizada en más de 851.220 millones de dólares, o el gigante Google, ahora denominado Alphabet con un valor de US$2 billones, sumas sin duda exorbitantes, y eso sin

ahondar en la gran influencia internacional que mantienen dichas compañías incluso en asuntos de política internacional, o el incesante desarrollo e innovación tecnológica que producen. Ahora, bien es cierto que muchas de dichas empresas tienen una relación con la innovación y desarrollo humano, también es cierto que, por el desarrollo de sus actividades, y el nivel de estas, generan un riesgo de comisión delictiva, como lo son los delitos contra el orden económico, corrupción de funcionarios, medioambientales, salud pública, y por supuesto delitos informáticos.

Ante dicho escenario, surge el derecho penal económico y de la empresa, como rama de las ciencias penales encargada de regular y procesar tanto al delincuente corporativo, o también denominado "delincuente de cuello blanco", como de establecer el tratamiento penal e imputación a la empresa o persona jurídica como colectivo, esto es frente a la abierta teoría de que la persona jurídica es susceptible a sanciones penales, es decir el fin del latinismo "*societas delinquere non potest*" que se traduce como "la sociedad no puede delinquir", por lo que la tendencia doctrinal y legislativa, hace posible hablar de un derecho penal de la empresa, surgiendo el *compliance*, del cual hablaremos más adelante, como herramienta de prevención y mitigación de riesgos penales (Abad, 2019).

En esa línea de ideas, es necesario precisar que los desarrollos dogmáticos relacionados al Derecho Penal y empresa corresponden a estudiarse al amparo del Derecho Penal Económico, no siendo lo mismo pero perteneciendo a este. En dicha línea, Caro Coria y Reyna Alfaro (2019), citando Tiedemann, conceptualizan que el Derecho Penal económico implica el conjunto de delitos relacionados a la actividad económica de la sociedad, y que transgreden las normas Estatales a fin de romper el orden económico. En un sentido más amplio, el Derecho Penal Económico no solo busca proteger el orden económico como tal,

sino también las actividades económicas, a fin de que se realicen dentro de la legalidad económica de mercado, y en protección de los derechos fundamentales.

En este punto es necesario explicar la diferencia doctrinal entre Derecho Penal Económico y Derecho Penal de la Empresa, en dichos términos Caro y Reyna, proponen que el concepto de Derecho Penal de la Empresa no solo debe entender como el estudio de la Responsabilidad Penal de la Persona Jurídica, la cual si bien es cierto tiene cierta aceptación legislativa, aún existen concepciones dogmáticas imperantes que la cuestionan; en base a ello proponen entender el Derecho Penal de la Empresa como a la lesión de bienes jurídicos cometidos por una empresa en afectación de terceros o de colaboradores de la empresa, no obstante entendido a la empresa no desde una concepción mercantilista o societaria, si no desde un concepto amplio de empresa como unidad económica que realiza actividad económica como tal.

La responsabilidad penal de las personas jurídica en el Perú.

Ante las nuevas formas de criminalidad, el Derecho Penal se encuentra en la necesidad de sancionar los delitos económicos y empresariales, así como incentivar su prevención. En base a lo anterior podemos decir que la persecución a una persona natural como tal, sin el involucramiento penal del ente colectivo al cual pertenece cuando el delito se comete en un escenario empresarial resulta insuficiente, por lo que la tendencia actual del Derecho Penal es perseguir del mismo modo a una persona natural como a una persona jurídica en un proceso penal, con las mismas garantías y sanciones y/o medidas que la ley permita imponer a las personas jurídicas (Abad, 2019).

Por otro lado, Caro Coria y Reyna Alfaro (2019), refieren la conveniencia político-criminal de la responsabilidad penal empresarial, al precisar que mediante un enfoque

político-criminal orientada a la función del Derecho Penal, la finalidad de proteger bienes jurídicos del derecho penal, ser vería mejor desarrollada al tener la posibilidad de imputar responsabilidad a una persona jurídica de forma directa. Para llegara a dicha conclusión deben tenerse en cuenta los datos revelados por parte de la criminología, ello a la luz de un estudio del Instituto Max Planck de Alemania, el cual reveló que el 80% de los delitos cometidos en Alemania estaban relacionados a actuaciones a favor de una empresa. Asimismo, es conocido los grandes efectos desestabilizadores de los grandes delitos económicos, como los conocidos casos de Enron o Madoff, el primero involucrados a manejos fraudulentos de información financiera, y el segundo a un fraude piramidal millonario.

Ahora bien, como mencionamos anteriormente, existen al menos tres fórmulas de atribución de responsabilidad a la persona jurídica, siendo estas: a) responsabilidad vicarial o heteroresponsabilidad, b) responsabilidad autónoma y c) el modelo mixto. En el primer modelo, denominado, modelo vicarial, heteroresponsabilidad o de transferencia de responsabilidad, la culpabilidad atribuida a la persona natural imputada se transfiere a la persona jurídica. Siendo los presupuestos generales a) que se haya cometido una infracción por parte de uno de los empleados de la organización, b) que dicha infracción normativa se haya cometido en ejercicio de sus funciones como parte de la organización, y c) que la infracción se haya cometido con la intención de obtener algún tipo de beneficio o ventaja para la persona jurídica, o en violación de sus obligaciones. Cabe mencionar que en varios sistemas (Reino Unido, Francia, Perú), no cualquier persona natural relacionada a la persona jurídica podría traer como consecuencia la responsabilidad de esta última, si no solo las conductas del denominado “cerebro” de la organización, como establece la doctrina del “alter-ego” anglosajón, donde solo determinadas personas físicas con facultad de dirección

o representación de la persona jurídica devienen en alter-ego de esta, por lo que sus conductas también serían las de la persona jurídica. Caso contrario se da en el modelo norteamericano, donde cualquier empleado o cualquier persona que obre en nombre de la organización, puede traer como consecuencia responsabilidad a la persona jurídica. Caro y Reyna (2019).

En el segundo modelo es el planteado desde la teoría de la culpabilidad de la persona jurídica, autorresponsabilidad, o responsabilidad por el hecho propio. En dicha doctrina, se tiene en cuenta la responsabilidad del ente colectivo basado en factores provenientes de la propia persona jurídica. Parte del concepto de esta postura es que la persona jurídica tendría capacidad de acción, y por lo tanto de la culpabilidad, entendiéndose que dicha capacidad de acción es la realizada por sus representantes o los que obren en nombre de esta, la cual, en base a la doctrina del alter-ego, estas serían consideradas acciones de la persona jurídica. Esta teoría también es denominada responsabilidad por el hecho propio. Caro y Reyna (2019).

El tercer modelo, es el modelo mixto, en el cual se reúnen los principales elementos de la responsabilidad vicarial y la responsabilidad autónoma, como lo es el concepto de transferencia de responsabilidad por la acción de determinados funcionarios o empleados de la persona jurídica, pero al momento de la gradualidad de la sanción se consideran aspectos de culpabilidad de la persona jurídica, como lo es la existencia de un programa de cumplimiento penal o criminal *compliance*, el cual dependiendo de su estándar podrá significar un atenuante de responsabilidad o un eximente de esta.

En el caso peruano, existen dos normas en materia penal aplicables a las personas jurídicas, la primera se encuentra regulada como las Consecuencias Accesorias del delito

aplicables a las Personas Jurídicas, regulado en el Art. 105 del Código Penal, que regula el modelo de heteroresponsabilidad o responsabilidad vicarial, y en contraste, el reciente marco de la Ley 30424 Ley que regula la responsabilidad administrativa de la persona jurídica, o responsabilidad autónoma. Pasaremos a explicar este último primera por temas metodológicos.

La Responsabilidad Administrativa de la Persona Jurídica Ley 30424

Como hemos referido, en el Perú el aforismo *societas delinquere non potest* que significa "la sociedad no puede delinquir", se ha mantenido como uno de los pilares doctrinales del derecho penal, no obstante, dicho paradigma jurídico fue al fin superado con la emisión de la Ley 30424, Ley que regula la responsabilidad administrativa de las Personas Jurídicas por el delito de Cohecho Activo Transnacional, publicada el 21 de abril del 2016, la misma que antes de su entrada en vigencia fue modificada por el Decreto Legislativo N.° 1352, de fecha 07 de enero de 2017, la cual modificó la denominada responsabilidad administrativa a otros delitos como lo es el cohecho estándar, el lavado de activos y financiamiento del terrorismo, siendo que dicha ley se encuentra vigente desde el 01 de enero del 2018, y que cuyo reglamento fue emitido mediante el Decreto Supremo N.° 002-2019-JUS de fecha 09 de enero de 2019.

Ahora bien, para desarrollar esta norma, existen diversos aspectos que incluso pueden resultar contradictorios en la técnica legislativa utilizada, así pues, Caro y Reyna, precisan que, en un primer término, podría entenderse que el principio de *societas delinquere non potest*, sigue vigente en el Perú, ello dado a que la norma que regula la responsabilidad de la persona jurídica la denomina taxativamente "responsabilidad administrativa". No obstante, existen críticas sustanciales al respecto, empezando que si bien se denominada

legislativamente "responsabilidad administrativa", esta no se da en sede administrativa, si no en sede penal, emitido por un juez penal mediante una resolución judicial, y dentro de un proceso penal con las garantías correspondientes, siendo de aplicación lo pertinentemente del Código Penal y Código Procesal Penal del 2004.

Ahora bien, en este punto será necesario hacer referencia al denominado "fraude de etiquetas" al denominar responsabilidad administrativa, a lo que, en palabras de Caro Coria, sería una responsabilidad penal corporativa. Sin embargo, cabe mencionar que la ley establece que solo será responsable administrativamente cuando el delito haya sido cometido por una persona física de las detalladas en el artículo 3° de la norma, aun cuando dicha lista pueda entenderse en sentido amplio, lo cual sería una muestra de una transferencia de responsabilidad o heteroresponsabilidad.

Por otro lado, y siendo de la misma opinión Caro y Reyna, en su articulado 4°, la ley regula expresamente que la responsabilidad administrativa de la persona jurídica es autónoma a la responsabilidad penal de la persona natural, y que la extinción de la responsabilidad de la persona natural, no enerva la responsabilidad de la persona jurídica. Por lo que se determina que, en esencia, no se trata de una responsabilidad meramente administrativa como consecuencia de un delito cometido por la persona física, siendo que debe existir una imputación y carga probatoria independiente contra la persona jurídica, siendo que la denominación de responsabilidad "administrativa" obedece masa criterios de conveniencia empresarial que jurídica, debido a que es más aceptable decir que una empresa ha sido sancionada administrativamente por un delito cometido por uno de sus trabajadores, a que una empresa haya sido sancionada penamente por un delito cometido por la organización, trayendo consigo un coste reputacional y comercial mucho mayor.

En base a lo anterior, podríamos advertir entonces que la norma vigente, la Ley 30424 mantiene los elementos más importantes tanto de la heteroresponsabilidad o responsabilidad penal corporativa derivada, como también de la responsabilidad autónoma o autorresponsabilidad. No obstante, debemos tener en claro el concepto de culpabilidad en la aplicación de la norma (si es que se le quiere ver desde un punto de vista penal). Dado que, si bien por un lado se advierte la imputación por transferencia de responsabilidad, también se acepta la atenuación o eximente de responsabilidad por la presencia de programa de cumplimiento o *compliance program*, siempre y cuando exista de forma previa a la comisión del delito, lo cual se entendería como una disminución de la reprochabilidad de la persona jurídica, reduciendo su culpabilidad. Este punto es especialmente relevante, dado que, para comprender una responsabilidad penal de la persona jurídica, debe entenderse un concepto de culpabilidad penal de la persona jurídica.

Características esenciales de la Ley 30424 Ley que regula la Responsabilidad Administrativa de la Persona Jurídica

Ya explicado el desarrollo dogmático de la norma bajo estudio, así como sus principales cuestiones problemáticas, corresponde explicar sus principales características, dentro de las -ya explicadas- encontramos las siguientes:

1) Conserva el principio de responsabilidad trasladada, en el cual el delito es cometido por la persona física que funge como representante, administrador de hecho, director, accionista o similar de acuerdo con el artículo 3° de la ley.
2) Regula la autonomía de la responsabilidad administrativa de la persona jurídica, independientemente de la responsabilidad de la persona física, así esta última haya sido absuelta o su responsabilidad penal haya sido extinguida.

3) Establece la responsabilidad administrativa atenuada de la persona jurídica ante la existencia de un programa de *compliance* previo a la comisión del delito, e incluso puede resultar en el eximente de responsabilidad de la persona jurídica.
4) De acuerdo con la redacción legislativa vigente, la ley solo es aplicable por la comisión de los siguientes delitos: lavado de activos, financiamiento del terrorismo, cohecho en todas sus modalidades, colusión, delito de tráfico de influencia.

Características esenciales del programa de cumplimiento o criminal *compliance program*.

Como se ha mencionado previamente, uno de los puntos más relevantes de la ley 30424 Ley que regula la responsabilidad administrativa de la persona jurídica, es el eximente de responsabilidad por existencia de un programa de cumplimiento, regulado en el artículo 17° de la norma, en dicho sentido, la norma precisa que la persona jurídica está exenta de responsabilidad por la comisión de los delitos comprendidos en su artículo 1° (cohecho genérico, cohecho activo transnacional, cohecho activo específico, lavado de activos, o financiamiento del terrorismo), si adopta e implementa en su organización, con anterioridad a la comisión del delito, un modelo de prevención (*compliance program*) adecuado a su naturaleza, riesgos, necesidades y características, consistente en medidas de vigilancia y control idóneas para prevenir los delitos antes mencionados o para reducir significativamente el riesgo de su comisión.

En dicho sentido, un programa de cumplimiento, o *compliance*, consiste en las normas éticas, controles y procedimientos internos en una empresa o persona jurídica en general, destinados a reducir los riesgos penales (riesgos de comisión delictiva) que puedan

generarse en el desarrollo de su actividad, garantizando el cumplimiento de las normas legales y éticas, así como de detectar y accionar contra los incumplimientos, todo ello buscando generar una cultura de cumplimiento y respeto a la norma (Clavijo, 2014).

Así pues, el artículo 17° precisa los elementos mínimos que tiene tener un modelo de prevención, los cuales son los siguientes:

Encargado de prevención y Oficial de Cumplimiento:

La figura del oficial de cumplimiento o *Compliance Officer* dentro de la doctrina penal aún es materia de debate, siendo que su posición implica una delegación de funciones de las funciones de vigilancia y control primigeniamente a cargo del empresario, siendo que, como su nombre lo dice, será el Oficial de Cumplimiento el encargado de todo el sistema de prevención o *compliance*, debiendo este velar por su correcta aplicación y la funcionalidad de los mecanismos de prevención y mitigación de riesgos. No es necesario que el encargado de prevención sea un abogado especialista en *compliance*, pero sí que este conozca bien la actividad económica, el modelo de negocio y los riesgos de su actividad.

Un punto importante es referencia a la responsabilidad penal del oficial del cumplimiento cuando se produzca un hecho delictivo dentro de la organización, y que este estaba en la posición de prevenir, ello basado en el deber de control y posición de garante que asume, por lo que, dependiendo de la legislación y la posición doctrinaria podríamos hablar de una comisión por omisión por parte del oficial de cumplimiento, el cual teniendo conocimiento o estando en la posibilidad de conocer de la comisión o posible comisión de un hecho ilícito, no comunicó ni lo mitigó en ejercicio de sus funciones.

Elaboración de mapa de riesgos (identificación, evaluación y mitigación de riesgos):

Dicha característica consiste en realizar un análisis de la persona jurídica a fin de obtener información destinada a poder realizar la elaboración e implementación de un programa de cumplimiento, ello consiste en identificar los riesgos que mantiene la empresa de acuerdo con su actividad, realizar una evaluación sistemática y multisectorial de los riesgos identificados, e implementar acciones de mitigación de riesgos de acuerdo a la información recolectada. De acuerdo con Caro y Reyna (2019), el análisis de riesgos consta de los siguientes pasos:

1) Fijación de objetivo: En este se debe determinar la actividad o giro de negocio de la empresa en la cual se irán a analizar los riesgos penales, ello a fin de implementar los específicos y correctos mecanismos de control.
2) Identificación de las posibles infracciones: En este punto, es preciso tener en consideración los riesgos de infracción a los cuales se encuentra expuesta la empresa de acuerdo con su actividad, dado que no será el mismo riesgo a la cual se encuentra expuesta una empresa de extracción de hidrocarburos a una empresa de construcción.
3) Probabilidad del riesgo: Identificado el objeto, y los riesgos a los cuales se encuentra expuesta la empresa dentro de sus actividades, es precio realizar un análisis de la probabilidad de que dicho riesgo de materialice en una infracción real (penal o administrativa). Ello ayudará a establecer mecanismos de control más eficientes de acuerdo con el nivel de probabilidad.
4) Evaluación del riesgo: Una vez medidas las probabilidades de materialización de riesgos, deben evaluarse las acciones a realizar para su mitigación, evaluando la necesidad de las acciones de acuerdo con un análisis de

preponderancia de riesgos, identificando que riesgos ameritan mayor atención que otros, teniendo como indicador su importancia, afectación o probabilidad de concreción.

5) Tratamiento del riesgo: Habiéndose identificado, evaluado y priorizado los riesgos, deben evaluarse los criterios y acciones para la disminución de dichos riesgos. Dichas acciones pueden versar sobre la prohibición de conductas en la empresa, o la implementación o mejora de mecanismos o procedimientos específicos que aumenten el control o disminuyan las probabilidades de infracción.
6) Revisión: Una vez realizados todos los pasos del mapa de riesgos y su implementación, la evaluación constante de los riesgos y de los mecanismos de prevención implementados debe ser constante, sobre todo cuando aparezcas nuevas infracciones no previstas, o los mecanismos de prevención implementados no hayan cumplido su cometido.

Canales y procedimientos de denuncia:

Conocido en la doctrina penal como "Whistleblowing" este elemento versa sobre los procedimientos que tiene la empresa o persona jurídica para que sus empleados, funcionarios, clientes, proveedores, y colaboradores en general puedan comunicar a su dirección o área y/o encargado correspondiente, las conductas antiéticas o de sospecha de posible infracción que se pudieran desarrollar dentro del funcionamiento de la empresa, según Henriksson (2019), es una herramienta, que permite a los empleados y personas en general, informar de forma confidencial las sospechas de mala conducta, informando a los directores de forma temprana sobre la posible comisión de actos de corrupción, fraude, acoso, y otros actos ilícitos.

Difusión, capacitación, evaluación y monitoreo continuos del modelo de prevención.

La difusión y capacitación del modelo de prevención tiene una motivación en esencia valorativa y de concientización de los empleados de la empresa sobre sus funciones y actuar dentro del modelo de prevención. Implica que los empleados tengan conocimiento de los mecanismos de prevención, procedimiento y códigos de conducta, así como los canales de comunicación disponible y formas de acción ante la presencia de actos sospechosos. Constituye una comunicación efectiva con los empleados sobre la existencia de problemas de cumplimiento y/o dificultades en su implementación o desarrollo. Por su lado, el monitoreo y evaluación periódica permite advertir la existencia de deficiencias o mejoras necesarias en el modelo de prevención, el mismo que debe ser sometido a una evaluación periódica a fin de asegurar su funcionalidad y efectividad. Cabe precisar, que tanto las capacitaciones y evaluaciones deben ser debidamente documentadas, a fin de tener un registro de la evolución del programa de prevención, a fin de tener una visión global del programa de cumplimiento.

Sanciones aplicables a las personas jurídicas y su naturaleza jurídica.

Una vez procesada y acreditada la responsabilidad administrativa de la persona jurídica por la comisión de ilícitos penales taxativos en su nombre, el juez penal a solicitud del fiscal, podrá imponer alguna o varias de las medidas administrativas reguladas en el artículo 5° de la ley, pudiendo ser: a) multa, b)inhabilitación (suspensión, prohibición de actividades específicas, suspensión para contratar con el estado), c) cancelación de licencias derechos, concesiones y otras autorizaciones d) clausura de locales y establecimientos temporal o definitivo e) Disolución de la persona jurídica.

Un punto relevante, sobre las medidas aplicables resulta que de una lectura sistemática de la ley 30424 y el artículo 105° del Código Penal correspondiente al capítulo de consecuencias accesorias del delito, estas serían casi las mismas, por lo que no habría mayor diferencia formal en su aplicación, variando solo en la cuantificación de la sanción y en los atenuantes intervinientes.

Sobre la naturaleza jurídica de estas medidas, existe un amplio debate en la doctrina penal, siendo que por un lado estas sanciones son tomadas como medidas de seguridad o medidas preventivas de la persona jurídica, con una esencia de medida administrativa, y otra parte en oposición a esta posición, se interpretan como sanciones de naturaleza penal, en base a la ausencia de una finalidad reparatoria y restitutiva patrimonial de la medida, y de que se encuentran sometida a contradicción y probanza en sede penal con las garantías procesales y constitucionales correspondientes.

Al respecto la Corte Suprema de Justicia, mediante el Acuerdo Plenario 07-2009/CJ-116 realizó el desarrollo dogmático de dichas medidas, tanto en el fundamento 11 y 12 de la citada, donde se concluye que las medidas aplicables a las personas jurídicas son una suerte de "consecuencias penales especiales", debido a que para su aplicación es necesario que la persona jurídica sea declarada judicialmente involucrada a la ejecución, favorecimiento u ocultamiento de un delito, sea por motivo de su actividad, administración, u organización, ellos justificado en activos y criminógenos defectos de organización, o una deficiente gestión de riesgos. Por otro lado, que la aplicación de dichas medidas significa una privación y restricción de derechos y facultades de la persona jurídica. Para finalizar, el Acuerdo Plenario concluye, que dichas medidas no pueden catalogarse como penas accesorias a imponerse a una pena principal al autor, como lo sería la inhabilitación, si no, que su calidad de accesoria, vicaria o paralela (responsabilidad por transferencia), es más una condición

normativa de aplicación (condición objetiva de procedibilidad), lo cual no enerva la naturaleza de pena de dichas medidas.

Sobre las consecuencias accesorias aplicables a la persona jurídica según el artículo 105° del Código Penal y diferencias con la Ley 30424

Ahora bien, como relatamos previamente, dentro de la normativa peruana existe otra fórmula de imputación para procesar penalmente a las personas jurídicas, ello en referencia de las consecuencias accesorias del delito amparadas en el Art. 105 del Código Penal Peruano, en cuyo terno se establece que si el hecho punible fuera cometido en ejercicio de la actividad de cualquier persona jurídica o utilizando su organización o estructura, sea para favorecer, encubrir o facilitar la comisión de un delito, dicha persona jurídica será pasible de imponérsele consecuencias accesorias del delito, también llamadas medidas de mitigación, o en palabras del Acuerdo Plenario 07-2099 sanciones penales especiales, las cuales, de acuerdo a la prognosis de sanción, puede ordenarse la suspensión o prohibición de actividades a la persona jurídica, la imposición de multas, la intervención judicial, e incluso la disolución de la misma. Como hemos precisado, las medidas establecidas en el artículo 105° son similares a las establecidas en la Ley 30424, siendo las principales diferencias esencialmente referidas a su naturaleza jurídica y requisitos de procedibilidad, propios de la responsabilidad vicarial pura.

Sobre su naturaleza jurídica, según la doctrina especializada, la aplicación de consecuencias accesorias a la persona jurídica no obedecería a un defecto de organización o deficiente gestión de riesgos, dado que la norma no contempla un eximente o atenuante de responsabilidad por la existencia de un modelo de prevención o *compliance program*, por lo cual no se podría hablar de elementos de culpabilidad de la persona jurídica por deficiente

gestión de riesgos para la aplicación de consecuencias accesorias del delito, si no, que se desarrolla el concepto de "peligrosidad objetiva" que emanaría de la persona jurídica por verse involucrada en actividades criminales, generando un riesgo no permitido en la sociedad.

En esa misma línea, y contrastando los modelos de procesamiento vigentes, la ley 30424 busca procesar y sancionar de forma autónoma a la persona jurídica, por la comisión de delitos taxativamente expresos en la norma, cometidos por sus funcionarios (sea representante, administrador de hecho, director, accionista o similar de acuerdo con el artículo 3° de la ley), por los delitos de cohecho genérico, específico y transnacional, tráfico de influencia, lavado de activos, y financiamiento del terrorismo, de los cuales la empresa, por causa de la comisión de dichos delitos, se hubiera visto beneficiada directa o indirectamente. Por el contrario, en el caso de las consecuencias accesorias, no necesita acreditarse un beneficio a favor de la persona jurídica, si no, solo que esta haya sido utilizada o instrumentalizada para cometer un delito (cualquiera de los amparados den el Código Penal y que no estén previstos en la ley 30424), independientemente de que si la empresa se benefició directa o indirectamente, si no que, basándose de forma focalizada en la instrumentalización criminal que ha sufrido la persona jurídica, sea para realizar, favorecer o encubrir el delito, esta se convierte en un ente criminalmente instrumentalizado, por ende en un ente peligroso, es decir, que denota una peligrosidad objetiva para la sociedad, dado que ya ha sido utilizado para fines delictivos.

Por otro lado, se diferencia de forma obvia y marcada en los requisitos de procedibilidad, siendo que para la imposición de consecuencias accesorias es requisito indispensable haber identificado al autor físico y que este sea sentenciado en un sentido condenatorio, radicando en ese aspecto el sentido vicarial de la norma, siendo que si por el

contrario la sentencia a la persona natural imputada resulta ser absolutoria, o se extingue su responsabilidad penal, la imposición de consecuencias accesorias a la persona jurídica involucrada será imposible, debido a la naturaleza procedimentalmente accesoria de la medida.

En relación con el catálogo de delitos por los que se puede imponer consecuencias accesorias a la persona jurídica en aplicación del artículo 105° del Código Penal; dicha norma no impone un catálogo números clausus de delitos, pudiéndose aplicar por la instrumentalización de la persona jurídica ante la comisión de cualquier delito del Código Penal, u otras leyes especiales.

Esta última diferencia sobre el catálogo de delitos, resulta especialmente importante, dado que los delitos informáticos regulados en la Ley 30096 Ley de Delitos informáticos, no se encuentran inmersos en el catálogo de delitos cerrados de la ley que regula la Responsabilidad Administrativa de la Persona Jurídica Ley 30424, por lo que no sería posible aplicar la responsabilidad autónoma ante la comisión de delitos informáticos en ambientes empresariales, lo cual consideramos es un error, por motivos que expondremos más adelante.

Procesamiento penal de la Persona Jurídica: Procedimiento de incorporación al proceso penal

Ya explicados los fundamentos dogmáticos de la atribución de responsabilidad de la persona jurídica y la normativa que la regula en el Perú, queda exponer la fórmula de procesamiento penal regulada y vigente en el Perú. Así pues, el Código Procesal Penal Decreto Legislativo 957, establece en sus articulados 90° al 93°, la incorporación de la persona jurídica al proceso penal, estableciendo que antes de finalizar la investigación

preparatoria, el fiscal deberá realizar un requerimiento de incorporación de la persona jurídica al proceso penal de manera formal ante el juez de investigación preparatoria, identificando plenamente a la persona jurídica, exponiendo los hechos que se le atribuyen (cadena de atribución), y los elementos de convicción que lo sustentan.

Un punto relevante, es que las disposiciones procesales citadas fueron pensadas en aplicación del artículo 105° del Código Penal, referente a las consecuencias accesorias aplicables a las personas jurídicas, no obstante, la Ley 30424, Ley que Regula la Responsabilidad Administrativa de la Persona Jurídica, carece de una regulación procesal específica, limitándose en su Tercera Disposición Complementaria Final, establecer como vía procesal para la investigación, procesamiento y sanción lo establecido en el Código Procesal Penal Decreto Legislativo 957° y sus normas complementarias. Sin embargo, la única regulación referente a la incorporación y procesamiento de las personas jurídicas en el Código Procesal Penal se encuentra en los artículos 91° al 93° referidos a la aplicación de consecuencias accesorias, por lo que, mediante la interpretación sistemática y teleológica de la norma, y por mandato legal, corresponde aplicar la Ley 30424 mediante los artículos 90° al 93° del Código Procesal Penal en la medida que sean pertinentes y de acuerdo con su naturaleza.

En dichos términos, ante el requerimiento fiscal de incorporación, sea para consecuencias accesorias, o responsabilidad administrativa, se convocará a audiencia de incorporación de la persona jurídica, donde el fiscal deberá exponer los hechos que justifican el procesamiento penal persona jurídica al proceso penal, esto es en primer término, que exista la potencialidad de aplicación de consecuencias accesorias, mediante indicios claros de una instrumentalización de la estructura empresarial de la persona jurídica para cometer ilícitos penales, para realizar, favorecer o encubrir el delito (Art. 91 CPP), o, en caso de la

Ley 30424, que se haya cometido un delito tipificado en la norma por uno de los sujetos establecidos y que dicho acto ilícito haya traído como consecuencia un beneficio ilícito a la persona jurídica.

En tal audiencia, la persona jurídica deberá apersonarse con su defensa técnica, asistiéndole todos los derechos y garantías procesales. Asimismo, de considerar mérito suficiente para proceder con la incorporación de la persona jurídica, el juez de investigación preparatoria emitirá resolución de incorporación de persona jurídica, exponiendo los fundamentos de mérito e incorporando formalmente a la persona jurídica al proceso.

Una vez incorporada la persona jurídica al proceso penal, esta deberá designar en el plazo de cinco días un apoderado judicial, quien será la persona física que representará a la persona jurídica ante el proceso penal, no pudiendo ser la misma persona natural que tenga calidad de imputada que haya cometido el delito (Art. 92 CPP).

Es necesario resaltar que una vez incorporada, a la persona jurídica le asisten todos los derechos y garantías procesales pertinentes, siendo los mismos que se aplica a la persona física, teniendo en cuenta la naturaleza jurídica diferenciada de la heteroresponsabilidad y la autorresponsabilidad (Art. 93°).

Iniciativa de reforma: Proyecto de Ley 5630/2020-CR Ley de seguridad informática y represión de los delitos informáticos

Con fecha 26 de junio del 2020, los parlamentarios Santillana Paredes Robertina, Combina Salvatierra Cesar Augusto, Acate Coronel Eduardo Geovanni, Carcausto Huanca Irene, Benavides Gavidia Walter, Pérez Mimbela Jhosept Amado, Quispe Suárez Mario Javier, Merino Lopez Omar, Gonzalez Cruz Moises, del grupo parlamentario Avanza País presentaron en la Primera Legislatura Ordinaria 2020 el Proyecto de Ley de Seguridad

Informática y Represión de los Delitos Informáticos - Proyecto de Ley 05630/2020-CR, iniciativa legislativa que buscar reformar por completo la normativa de delitos informáticos vigente, derogando la Ley 30096 - Ley de delitos informáticos, modificada por la ley 30171, subsanando vacíos de la anterior norma (actualmente aún vigente), no limitándose solo a tipificar conductas, sino también estableciendo medidas de prevención de vulneraciones de ciberseguridad tanto en transacciones públicas o privadas en el ciberespacio.

Dicho proyecto establece principios regulatorios de transparencia en el comercio electrónico, regulando los términos y condiciones de bienes o servicios ofertados por internet, y estableciendo normas que permitan una mayor seguridad de la información y experiencia del usuario. Por otro lado, en su lado procesal, regula en sus términos "PROCEDIMIENTOS DE INVESTIGACIÓN CRIMINAL DE LOS DELITOS INFORMÁTICOS", haciendo referencia a las técnicas especiales de investigación de forma más detallada que su predecesora, a la luz del Código Procesal Penal (2004) y nomas conexas, así como detallando medidas especiales de la materia como el Bloqueo de Dominio DNS.

Ahora, uno de los aspectos más relevantes es el capítulo referente a la "RESPONSABILIDAD ADMINISTRATIVA DE LA PERSONA JURÍDICA", siendo esta la novedad más importante, y regulándola en el artículo 16° del proyecto de ley. Este aspecto es especialmente importante, siendo que utilizando los mismos términos de la Ley 30424 - Ley de Responsabilidad Administrativa de la Persona Jurídica (considerada por gran parte de la doctrina como penal), dicha norma regula la responsabilidad administrativa autónoma de la persona jurídica por la comisión de delitos informáticos cometidos por sus funcionarios, administradores, representantes de hecho o derecho, o personas naturales vinculadas, y que se hubieran cometió en nombre o beneficio de la persona jurídica.

Cabe precisar que la norma inicia su regulación precisando que la atribución de responsabilidad es independientemente de que sea o no una persona jurídica proveedora de servicios (entendemos de internet o servicios digitales, redes o afines), regulando así la pasibilidad de responsabilidad de cualquier empresa sin importar su actividad y que cometa delitos informáticos.

En ese mismo sentido, la norma en su artículo 16.3 también ampara el eximente de responsabilidad de la persona jurídica ante dos situaciones concretas, siendo estas 1. Cuando las personas naturales señaladas anteriormente y que hubieran cometido el delito directamente hubieran actuado en provecho propio o en beneficio de un tercero; y 2. Cuando la persona jurídica haya adoptado con anterioridad a la comisión del delito, un modelo de prevención (*compliance* penal), de acuerdo a su naturaleza, necesidades, riesgos y características, que en el caso concreto, sería un modelo de prevención de seguridad informática, también llamado, *compliance* digital o *cibercompliance*.

Sobre las sanciones aplicables, la norma nos deriva en las estipuladas en la Ley 30424, y que ya fueron precisadas anteriormente.

Derecho comparado: Normativa internacional

Dentro de la normativa internacional, es necesario citar el ejemplo español, siendo que desde el año 2010 con la LO 5/2010 de reforma del Código Penal Español, en su artículo 31bis regula la Responsabilidad Penal de las Personas Jurídicas, el cual al igual que el modelo peruano, es un modelo mixto de atribución de responsabilidad en la línea de la doctrina del *alter ego.* Asimismo, un punto relevante, es que su catálogo *numerus clausus* de delitos si ampara los delitos informáticos regulados en el artículo 264.4 del Código Penal Español.

En Latinoamérica, de forma reciente con fecha 20 de junio del 2022 em Chile, se emitió la Ley N° 21.459, como su nueva ley de delitos informáticos, adaptándose así al Convenio de Budapest, la misma que en su artículo 21° modifica la Ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas en Chile, incluyendo en su catálogo de delitos los delitos informáticos. Cabe mencionar que la Ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas en Chile también mantiene un modelo mixto de atribución de responsabilidad.

Por otro lado, en Alemania, aún se encuentra en debate el principio *societas delinquere non potest* dado que aún es rechazada en su normativa la responsabilidad penal de la persona jurídica, aplicándose en su lugar el Derecho de Contravenciones contra personas jurídicas, las cuales tienen una naturaleza administrativa sancionadora. Cabe mencionar que dicha posición se encuentra en un extenso debate dogmático.

En el caso italiano, se tiene el Decreto Legislativo 231/2001 que regula la responsabilidad administrativa de la persona jurídica, (muy parecido al modelo peruano). La misma que de forma reciente fue modificada por el Decreto Legislativo 184/2021, que implementó la Directiva de la UE 2019/713 de la Unión Europea, orientada a fortalecer la lucha contra el fraude y la falsificación de medios de pago en el viejo continente, incorporando en su normativa el delito de fraude informático.

De lo expuesto, hemos advertido el estado de la cuestión en lo que es responsabilidad penal de la persona jurídica en el Perú y su procesamiento penal relacionado a los delitos informáticos, lo cual nos servirá como punto de partida conceptual.

1.2. Antecedentes de investigación

A fin de exponer de forma clara el estado la técnica, mencionaremos algunos estudios previos relacionados al tema de estudio, tanto a nivel nacional como internacional.

1.2.1. Antecedentes Internacionales

Navas y Jaar (2018), en su artículo científico "La responsabilidad penal de las personas jurídicas en la jurisprudencia chilena", concluyen que los tribunales chilenos vienen aplicando concurrentemente los elementos establecidos por la Ley N° 20.393 que regula la responsabilidad penal de la persona jurídica en la normativa chilena. No obstante que en la jurisprudencia nacional no se ha verificado que las personas que ostenten los cargos de dirección, administración o representación, realmente (de forma material) ejerzan los cargos de administración y supervisión dentro de la empresa, ni tampoco se habría profundizado las razones o fundamentos por los cuales el delito fue cometido en interés directo de la persona jurídica, o solo a interés de la persona natural. Agrega que otro de los requisitos de la normativa chilena es que la comisión delictiva haya sido consecuencia del incumplimiento de los deberes de dirección y supervisión de la persona jurídica, lo que traería como consecuencia de que toda persona jurídica que no tenga un modelo de prevención estaría incumplimiento sus deberes de dirección y supervisión.

Rayón (2018), en su artículo científico de la Universidad Complutense de Madrid, titulado "Los programas de cumplimiento penal: origen, regulación, contenido y eficacia", concluye que, en el actual sistema de responsabilidad criminal de la persona jurídica, los administradores, y directivos de empresas deben adoptar las medidas necesarias para que sus organizaciones cumplan con la normativa legal aplicable, implementando los modelos de control adecuados para la prevención de delitos. Asimismo, es necesario realizar la evaluación riesgos de la empresa, o mapa de riesgos, de acuerdo con la actividad económica

de la empresa, para así identificar cuáles son los riesgos específicos a los cuales se encuentra expuesto penalmente.

Mañas (2016) en su trabajo de investigación de tesis de grado de la Universidad de Barcelona, titulado "La responsabilidad penal corporativa y cibercriminalidad", menciona que el desarrollo y proliferación del internet ha traído como consecuencia un riesgo latente a las organizaciones, principalmente delitos informáticos "con una probabilidad de ocurrencia del 37% a escala mundial y de un 24% a nivel estatal (PwC, 2016); luego, cada vez está teniendo más relevancia la seguridad de la información en el contexto empresarial". Siendo una necesidad la implementación de políticas de prevención de riesgos.

Posada (2017), en su artículo de investigación titulado "El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual", concluye que los grandes cambios del mundo contemporáneo, el cual al determinado el surgimiento de nuevos riesgos criminógenos como fenomenologías penales. De este modo los delitos informáticos se presentas como conductas ilícitas en ambientes virtuales, como los sistemas digitales y el ciberespacio. Mencionando que se busca la protección de bienes jurídicos de naturaleza netamente digital o informática y también los bienes jurídicos intermedios en delitos informáticos pluriofensivos.

Mayer y Oliver (2020), en su trabajo de investigación de la Revista Chilena de Derecho y Tecnología, titulado "El delito de fraude informático: Concepto y delimitación", concluyen que los problemas de imputación penal en los delitos de naturaliza netamente informática, como el hacking o phishing, en el cual debe adaptarse la teoría del delito

convencional y el itercriminis (camino del delito) a la comisión de delitos informáticos, para así diferenciar los actos neutros, actos preparatorios y actos de consumación del delito.

Fernández Días, (2018), en su artículo de investigación titulado "La amenaza de las nuevas tecnologías en los negocios: El ciberespionaje empresarial", precisa que el auge de las nuevas tecnologías ha traído nuevas formas de violar bienes jurídicos protegidos, citando como ejemplo el ciberespionaje en el mundo empresarial, y que "estas irrumpen en el mercado, desestabilizándolo, mediante injerencias ilícitas en el capital inmaterial más vulnerable de las empresas, el que constituyen sus secretos".

1.2.2. Antecedentes nacionales:

Blozziers (2018), en sus tesis de maestría titulada "El delito informático y su incidencia en la empresa bancaria", concluye que la afectación de los delitos informáticos a las empresas genera una afectación relevante en términos económicos, dado que en los casos de empresas bancarias, cuando sus clientes son afectados por delitos informáticos de fraude, la confianza de sus clientes se ve afectada de forma casi irremediable, sin mencionar las consecuencias penales y civiles que traerá como consecuencia.

Espinoza (2017), en su tesis de grado titulado "Derecho Penal Informático: Deslegitimación del poder punitivo en la sociedad de control", concluye en definir al Derecho Penal Informático como "el saber jurídico penal que, mediante la interpretación de leyes penales sobre Delitos Informáticos, propone a los agentes jurídicos un sistema reductor del poder de vigilancia del poder punitivo en la sociedad de control", ello con la intención de proteger los espacios de privacidad y las libertades digitales, en observancia de los límites intrínsecos.

Reyna (2016), en su artículo de investigación "Criminalidad informática, crimen organizado e internacionalización del delito", concluye que, ante el reto de la criminalidad organizada informática, se presentan serias dificultades para la persecución penal, sobre todo en la dificultad actos de investigación informática, por lo que es necesario un trabajo conjunto en entre el Ministerio Público y la División de Investigación de Delitos de Altas Tecnologías (Divindat)

García (2012), en su artículo de investigación titulado "Esbozo de un modelo de atribución de responsabilidad penal de las personas jurídicas", concluye que la atribución de responsabilidad a la persona jurídica solamente como consecuencias accesorias, deviene en insuficiente, al estar limitado a la persecución y procesamiento de la persona física. Por lo que esta naturaleza accesoria y vicarial, si bien podría reducir o eliminar la peligrosidad de la persona jurídica, no satisface la misión actualmente encomendada al Derecho Penal.

Caro (2020), en su artículo denominado "Imputación objetiva y *compliance* penal", resalta la importancia de una debida diligencia (due diligence) del empresario o miembro del órgano de administración, para que se considere el eximente de responsabilidad penal/administrativa de la persona jurídica, y que, en efecto, dicha debida diligencia se manifiesta en la implementación de un programa de *compliance* o de prevención del delito, que sea eficiente y eficaz, con una aplicación material en la cultura corporativa de la persona jurídica, es decir un control efectivo de las medidas de mitigación de riesgo.

1.3. Formulación del problema

1.3.1. Problema general: ¿Existe un adecuado procesamiento penal de la persona jurídica involucrada a la comisión de delitos informáticos en el Perú al año 2022?

1.3.2. Problema específico 1: ¿Qué elementos de juicio deben valorarse para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos informáticos?

1.3.3. Problema específico 2: ¿Cuál sería la fórmula de procesamiento penal adecuado para incorporar y procesar a una persona jurídica involucrada en la comisión de delitos informáticos?

1.4. Objetivos

1.4.1. Objetivo general: Determinar si existe un procesamiento penal adecuado de la persona jurídica involucrada a la comisión de delitos informáticos en el Perú al año 2022

1.4.2. Objetivo específico 1: Analizar qué elementos de juicio deben valorarse para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos informáticos

1.4.3. Objetivo específico 2: Proponer la fórmula de procesamiento penal adecuada para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos informáticos.

1.5. Supuestos de objetivos.

1.5.1. Supuesto de objetivo general: En el Perú no existe un procesamiento penal adecuado de personas jurídicas que se vean involucradas en la comisión de delitos informáticos.

1.5.1. Supuesto de objetivo específico 1: Los elementos de juicio que deben valorarse para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos informáticos son a) Identificación plena de la persona jurídica, b) Delito cometido dentro de su actividad empresarial, utilizando a la persona jurídica para realizar, favorecer o encubrir el delito c) Persona natural que ejerza funciones de dirección administración o representante que haya cometido el delito materialmente.

1.5.1. Supuesto de objetivo específico 2: La fórmula de procesamiento penal adecuada para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos informáticos en el Perú, es que la ley 30424 (Ley que regula la responsabilidad administrativa de la persona jurídica) incluya dentro de su catálogo de delitos a los establecidos en la Ley Nº 30096 "Ley de delitos Informáticos" y sus modificatorias.

1.6. Justificación

1.6.1. Justificación del objetivo general: La presente investigación se justifica teóricamente, dado que aportará al conocimiento jurídico posiciones sobre la correcta fórmula de procesamiento penal de la persona jurídica involucrada en comisión de delitos informáticos en el Perú. Su importancia radica en que cada vez se presentan más casos de delitos relacionados a empresas, sumado al auge de delitos informáticos, y al radicar en tipos penales novedosos en el Perú o de reciente manifestación en la realidad, no existe mucha difusión de su contenido y menos aún de su correcto procesamiento, siendo un campo inexplorado en la casuística peruana y las previsiones legislativas, por lo que buscará aportar conocimiento teórico al respecto, brindando a los operadores del derecho bases teóricas para el tratamiento de casos relacionados a personas jurídicas involucradas en la comisión de delitos informáticos, así como una propuesta de modificatoria legislativa al legislador penal para un adecuado procesamiento de estos casos.

La presente investigación será de utilidad teórica a todos los operadores jurídicos, teniendo en cuenta el incremento de la cibercriminalidad y el desarrollo corporativo imperante, siendo de suma importancia entender su tratamiento y procesamiento penal más allá de la persona natural.

Por lo anterior, el presente trabajo enriquecerá la doctrina en la materia, logrando mayor debate sobre el procesamiento penal de la persona jurídica y los delitos informáticos, el cual es un tema de desarrollo vigente.

1.6.2. Justificación del objetivo específico 1: Radica en que es necesario conocer cuáles son las valoraciones o criterios que deben valorarse para procesar penalmente a una persona jurídica involucrada a delitos informáticos, a fin de identificar la línea general de criterios esenciales de procesamiento.

1.6.3. La justificación del objetivo específico 2: Radica en la importancia que tiene fórmula de procesamiento penal adecuado de una persona jurídica involucrada en la comisión de delitos informáticos, siendo que, en base al desarrollo legislativo vigente, consideramos que el procesamiento previsto en la actualidad resultaría ineficiente

1.7. Hipótesis

En referencia a la hipótesis, Espinoza Freire (2018), explica que las hipótesis son explicaciones tentativas de un fenómeno, explicadas a modo de proposiciones. Dicho con otras palabras, busca dar una solución o respuesta a la problemática expuesta, la cual será respondida al final de la investigación de forma positiva o negativa. Con respecto a la presente investigación, la misma no requiere una respuesta apresurada o solución comprobable a los problemas expuestos, toda vez que versa sobre un tipo de investigación de índole cualitativo que no amerita demostración alguna, limitándose a analizar normas legales, doctrina, jurisprudencia y opiniones de expertos. Al respecto, Ramos Flores (2012), precisa que las investigaciones cualitativas por lo regular no formulan hipótesis antes de recolectar datos, por el contrario, su naturaleza es inducir la misma mediante la recolección y el análisis de datos. Asimismo, el mismo autor precisa que las investigaciones de carácter exploratorio no formulan hipótesis. Al respecto, y como se detallará en la parte metodológica, la presente investigación tiene carácter exploratorio, siendo que trata de

recolectar y analizar datos sobre situaciones jurídicas no estudiadas con anterioridad, como lo es el procesamiento penal de personas jurídicas involucradas a delitos informáticos, situación que a la fecha tampoco se ha dado en la casuística peruana, lo cual hace que sea una investigación teórica, cualitativa y exploratoria que no requiere hipótesis.

CAPÍTULO II: METODOLOGÍA

2.1. Tipo de investigación

Según el nivel y grado de alcance, la presente investigación se detalla como una investigación exploratoria, siendo que el problema de estudio no ha sido suficientemente estudiando, y constituye un primer acercamiento directo al objeto de estudio, buscando delimitar las condiciones existentes y posibles soluciones (Altuna, 2018), por cuanto la presente investigación, versa sobre la responsabilidad penal de las personas jurídicas y su procesamiento penal, tema de reciente legislación y poca aplicación en nuestro ordenamiento jurídico, lo cual se suma a su relación con los delitos informáticos, teniendo a entes colectivos como sujetos activos de un cibercrimen, la misma que es una figura no estudiada ni vista antes en la academia jurídica peruana.

Según el propósito de la investigación, el presente trabajo constituye una investigación básica, denominada también pura o fundamental, siendo que busca el desarrollo o progreso científico, aportando conocimiento teórico, no preocupándose por la aplicación práctica del mismo (Zorrilla, 1993, en Altuna, 2018). Siendo que como es el caso, la presente investigación es netamente teórica; dado de que a la fecha, no existen procesos o investigaciones penales formalizadas, que hayan identificado a una persona jurídica como presunto responsable de delitos informáticos, al mismo tiempo que para que se ponga en práctica lo expuesto es necesaria una reforma legislativa sobre la inclusión de delitos informáticos en la ley especial que regula la Responsabilidad Administrativa de la Persona Jurídica Ley 30424, la misma que es competencia exclusiva del Congreso de la República, a la par que sería necesaria la comisión de un hecho ilícito (comisión de un delito informático mediante el uso de una persona jurídica), lo cual escapa en absoluto de la presente

investigación, por lo que, de acuerdo a la base teórica expuesta, se limitará al desarrollo teórico y progresivo científico del objeto de estudio.

Asimismo, por el enfoque, el presente trabajo es de enfoque cualitativo, siendo que se centra en el estudio y comprensión de fenómenos externos, a fin de explicarlos en base a sus características, elementos y espacio de desarrollo. Precisa del análisis de datos con el objetivo de explicar una posición jurídica, prescindiendo de estadísticas o cantidades exactas. En dicho sentido, sobre el enfoque de investigación cualitativo, Martínez M. (2006), explica que este enfoque busca identificar la naturaleza, estructura, razón de comportamiento y manifestación del objeto de estudio, por lo que lo cualitativo es el todo integrado, y lo cuantitativo es un aspecto en especial, complementándose ambos enfoques entre sí. Por lo que el aporte de la presente investigación será teórico, cualitativo sin hipótesis necesaria, toda vez que analizará sistemática e integralmente una parte del Derecho, buscando aportar un análisis hermenéutico al conocimiento jurídico sobre instituciones del Derecho Penal, siendo imposible su comprobación al análisis conductas ilícitas.

2.1.1. Diseño de investigación:

La presente investigación de acuerdo con sus objetivos de investigación tiene un diseño no experimental de tipo transversal, al respecto Álvarez Risco (2020) señala que para realizar toda investigación y dar respuesta a los objetivos de investigación e hipótesis en caso se tenga, deberá considerarse una estrategia de investigación, la cual recibirá el nombre de diseño de investigación. En relación con el diseño de investigación no experimental de tipo transversal, precisa que este diseño se da cuando no existe una manipulación de las variables por parte del investigador, al mismo tiempo que re realiza un análisis de las variables en un momento específico, sin evaluar su evolución. En dicho sentido, la presente investigación, no realizará manipulación alguna de las variables, referidas al procesamiento penal de las

personas jurídicas, y su relación con los delitos informáticos, limitándose a su estudio y análisis sin manipulación de estas, el cual se realizará en el momento exacto de re la recolección y procesamiento de datos, resaltado cual es el estado actual para así dar respuesta a los objetivos de investigación, sin evaluar el desarrollo de las variables en el tiempo.

2.2. Población y muestra

Tabla 1

La población y muestra

Población A1
La población del cual se recogerán los datos que servirán de material para la presente investigación, será la jurisprudencia del Poder Judicial del Perú, referente a la incorporación de la persona jurídica al proceso penal para la imposición de consecuencias accesorias (heteroresponsabilidad – artículo 105° C.P.), dentro del Sistema Especializado en Delitos de Corrupción de Funcionarios, siendo que dicho sistema especializado es el único que a la fecha viene emitiendo jurisprudencia sobre la incorporación y procesamiento de personas jurídicas en procesos penales, por lo que es imperativo el análisis de dichos pronunciamientos a fin de obtener los criterios generales de incorporación de una persona jurídica por hechos delictivos cometidos por sus funcionarios.
Muestra A1

La parte de la población a analizar, es decir, a muestra, versará de 08 resoluciones y recursos que resuelven un requerimiento de incorporación de una persona jurídica al proceso penal, divididas de la siguiente forma:

- 05 resoluciones del Primer Juzgado de Investigación Preparatoria Nacional
- 03 resoluciones de la Sala Penal de Apelaciones Especializada en Delitos de Corrupción de funcionarios.

Población A2

La población se constituirá de abogados peruanos especializados en Derecho Penal Económico y Derecho Penal de la Empresa.

Muestra A2

La muestra, versará de 08 abogados peruanos especializados en Derecho Penal Económico y de la Empresa, siendo los siguientes:

Tabla 2

Muestra de entrevistados

N.°	Nombres y apellidos	Profesión o cargo
01	Dino Carlos Caro Coria	Estudios de Derecho en la Pontificia Universidad Católica del Perú (1987 – 1993). Título de Abogado por la Pontificia Universidad Católica del Perú (abril 1994). Estudios de Maestría en Derecho Constitucional en la Pontificia Universidad Católica del

		Perú (marzo – julio 1995). Becario de la Agencia Española de Cooperación Internacional (octubre 1995 – junio 1998). Estudios de Doctorado en Derecho Penal en la Universidad de Salamanca-España (octubre 1995 – junio 1997). Estudios de Postgrado en Derecho Constitucional en la Universidad de Salamanca (enero de 1997). Estancia de investigación en el Instituto Max Planck para el Derecho Penal Extranjero e Internacional (Max Planck Institut für Ausländisches und Internationales Strafrecht) de Freiburg im Breisgau-Alemania (1997). Grado de Doctor en Derecho por la Universidad de Salamanca-España (mayo 1998), tesis reconocida por la Universidad de Salamanca con Premio Extraordinario de Tesis Doctorales (diciembre de 1998).
02	Luis Miguel Reyna Alfaro	Estudios de Derecho en la Universidad de San Martín de Porres (1992 – 1997). Título de Abogado por la Universidad de San Martín de Porres (1998). Estudios de Maestría en Ciencias Penales en la Universidad Nacional Mayor de San Marcos.

		Becario de Formación Permanente de la Fundación Carolina (2008). Estancia de investigación en el Departamento de Derecho Penal de la Universidad de Granada (2008). Experto en Criminología por la UNED- España (2012).
03	Virginia Naval	Estudios de Derecho en la Universidad de San Martín de Porres (2008 – 2013). Título de Abogada por la Universidad de San Martín de Porres (2014). Egresada de la Maestría en Ciencias Penales en la Universidad de San Martín de Porres (2017). Programa de Estudios Avanzados en Derechos Humanos y Derecho Internacional Humanitario en American University Washington College of Law (2011) Abogada Senior del estudio Caro & Asociados. Gerente de Cumplimiento de la Asociación Peruana de *Compliance* (desde mayo de 2019 – a la actualidad)

		Investigadora del Centro de Estudios de Derecho Penal Económico y de la Empresa – CEDPE
04	Fernando Ikehara Veliz	Bachiller por la Pontificia Universidad Católica del Perú (2010) Abogado por la Pontificia Universidad Católica del Perú (2012) Certificación de Especialista en Cumplimiento Normativo en Materia Penal por la Universidad Castilla La Mancha – España (2017) Magister en Derecho Penal por la Pontificia Universidad Católica del Perú (2019)
05	Daniel Ernesto Peña Labrín	Magíster en Derecho Penal por la Universidad Nacional Federico Villarreal, Abogado y Licenciado en Sociología; Segunda Especialidad en Derecho Informático por la Universidad Inca Garcilaso de la Vega.
06	André Sota Sánchez	Es abogado por la Universidad de San Martín de Porres (Perú). Maestría en Ciencias Penales por la Universidad de San Martín de Porres (Perú). Título de Especialista en prevención y represión del blanqueo de dinero, responsabilidad criminal de las personas jurídicas y fraude fiscal, por la Universidad de Santiago de Compostela (España). Título de

		Especialista en *Compliance* y Buenas Prácticas Corporativas, por la Universidad del Pacífico (Perú). Título de Especialista en *Compliance*, por Aenor (España)
07	Carlos Quisse Sanchez	Abogado por la Universidad Nacional de Trujillo, con estudios de pregrado concluidos en la Universidad Complutense de Madrid, como becario Santander, en materias de Derecho Penal y Derecho Penal Económico. Abogado Asociado de Caro & Asociados e investigador del Centro de Estudios de Derecho Penal Económico y de la Empresa.
08	Manuel Ibarra Trujillo	Abogado por la Universidad Nacional Federico Villarreal, Magister en Gestión Pública, Arbitro Comercial y Gerencial nacional e internacional. Docente universitario y ponente nacional e internacional en temas de Derecho Constitucional.

2.3. Técnicas e instrumentos de recolección y análisis de datos

Técnica:	
ANÁLISIS DOCUMENTARIO	**ENTREVISTA A EXPERTOS**
Para la primera técnica, se utilizará el análisis documental, es decir	Para la segunda técnica se utilizará la técnica de entrevista

el análisis razonado y sistematizado de datos escritos en textos académicos o jurisprudenciales. Según Dulzaides y Molina (2004), el análisis documental, es una forma de investigación técnica, basa en el conjunto de operaciones intelectuales destinadas a sistematizar y procesar información documentada, para facilitar su comprensión analítica. Dicha técnica de evaluación documental será empleada para realizar un correcto análisis jurisprudencial, destinado a seleccionar criterios judiciales. En efecto, se procederá con la selección de determinada jurisprudencia aplicable al objetivo de investigación, donde se analizarán los criterios aplicados por los jueces peruanos, a fin de fallar en un determinado sentido. Del análisis conjunto y sistemático de dichas resoluciones judiciales, se advertirá un patrón específico de criterios judiciales,	mediante el formulario de preguntas orientadas a dar una respuesta a cada objetivo de investigación, a fin de que los expertos de la materia brinden su opinión de forma libre e ilimitada, teniendo en cuenta su preparación académica y experiencia en el tema. En dicho sentido, la técnica de entrevista, según Hernández Sampieri (2014) las entrevistas como herramientas de recolección de datos cualitativos se emplean cuando el problema a investigar es demasiado complejo o difícil de observar, sea por dificultades fácticas o éticas; siendo que al ser la presente investigación sobre aspectos procesales penales, y más aún cuando las situaciones jurídicas que se investigan a la fecha no han tenido mayor desarrollo judicial, la entrevista a expertos resulta idónea.

siendo esta la información que servirá para análisis de los resultados.	
Instrumento	
Ficha de análisis documentario	Ficha de entrevista a expertos

Métodos

A fin de realizar una investigación con la más pulcra rectitud metodológica, se pasará a definir conceptualmente los tipos de métodos aplicables:

Método hermenéutico:

Podemos definir el método hermenéutico, como la teoría general de la interpretación y comprensión, es decir, busca entender procesos cualitativos e interpretar y comprender las razones del comportamiento humano (Ruedas, 2009)

En dicho sentido, nuestra investigación será de enfoque hermenéutico, toda vez del análisis jurisprudencial realizado, se realizará una interpretación de los criterios valorativos jurisdiccionales, intentando comprender los elementos valorados empleados por la judicatura nacional en referencia al objetivo de la investigación. En dicho sentido, será una investigación íntegramente cualitativa.

2.4. Procedimientos

2.4.1. Procedimientos de recolección de datos

Análisis Documentario	Entrevista a expertos

El proceso de investigación inició con la búsqueda de jurisprudencia relevante y actual sobre incorporación de persona jurídica al proceso penal, recabándose del Sistema Especializado en Delitos de Corrupción de funcionarios, siendo que, debido a los casos mediáticos de corrupción donde se ven implicadas empresas constructoras, se ha procedido a requerir la incorporación de estas al proceso penal, generan jurisprudencia rica y actualizada al respecto.	El proceso de selección de entrevistados se realizó mediante la identificación de especialistas en Derecho Penal de la Empresa y Legal Tech, y de Derecho Informático en el Perú, teniendo en cuenta su experiencia en la materia, nivel académico y prestigio reconocido. Posterior a ello se realizó las solicitudes de entrevista por correo electrónico y WhatsApp, brindando facilidades de entrevista escrita y reunión por Zoom, de los cuales 05 entrevistados por temas de agenda optaron por la entrevista escrita, y 03 por entrevista vía zoom, realizándose la transcripción correspondiente.
Las etapas fueron las siguientes:	**Las etapas fueron las siguientes:**
• Búsqueda jurisprudencial • Clasificación de jurisprudencia • Análisis de criterios aplicados • Exposición de criterios especialmente relevantes.	• Identificación de abogados especialistas en Derecho Penal de la Empresa y Legal Tech. • Coordinación con cada uno de los entrevistados • Realización de entrevista

	• Transcripción y análisis de entrevistas realizadas.

2.4.2. Procedimientos de análisis de datos

Método de análisis jurídico:

El análisis jurisprudencial aplicó el método hermenéutico

Hermenéutico: Se analizará e interpretará los criterios de evaluación para la incorporación de la persona jurídica al proceso penal, y de ello se interpretará la aplicación de dichos criterios a los delitos informáticos. Del mismo modo se analizarán las posiciones doctrinarias de los entrevistados, en referencia al adecuado modelo vigente de procesamiento penal de personas jurídicas relacionada a delitos informáticos.

2.5. Aspectos éticos

La presente investigación ha mantenido un respeto irrestricto a las normas legales y éticas, especialmente en los siguientes campos.

Ética académica y reserva de la información: La jurisprudencia analizada, y las entrevistas llevadas a cabo tienen una finalidad netamente académica, guardando las reservas y cuidados necesarios al versar sobre casos controversiales.

Propiedad intelectual: Se ha citado adecuadamente toda idea o material utilizado para la presente investigación en formato APA, haciendo especial uso del a cita paráfrasis.

Objetividad científica: Las valoraciones o posiciones son puramente académicas en base a un análisis hermenéutico y sistemático del derecho aplicable, excluyendo opiniones o valoraciones personales ajenas a la investigación.

CAPÍTULO III: RESULTADOS

3.1. Hallazgos de la técnica de investigación:

De acuerdo con la aplicación de las técnicas de investigación mediante los instrumentos utilizados de acuerdo con los estándares académicos correspondientes, a continuación, se expondrán los resultados empezando por las entrevistas a expertos y luego con el análisis documentario, dando respuesta al objetivo general y los dos objetivos específicos.

En relación con el Objetivo general: Determinar si existe un procesamiento penal adecuado de la persona jurídica involucrada a la comisión de delitos informáticos en el Perú al año 2022.

Asimismo, se plantearon las siguientes preguntas en relación con el objetivo general:

- A su criterio ¿Considera que Perú se encuentra preparado para procesar penalmente a una persona jurídica involucrada en la comisión de delitos informáticos?
- A su criterio, ¿Cuál es el impacto que sufre la persona jurídica involucrada en un proceso penal?

Al respecto se obtuvieron los siguientes resultados:

Entrevista

Tabla 3

Hallazgo N.° 1

Entrevistado	Respuestas
Carlos Dino Caro Coria	Precisa que, independientemente del delito, porque al ser delitos

	informáticos, el tratamiento sería el de consecuencias accesorias, la legislación actual de procesamiento de personas jurídicas es muy genérica e incipiente, y tiene grandes vacíos en lo que es la imputación a la persona jurídica y sus garantías. Parte de estos vacíos son, por ejemplo, el derecho a la no autoincriminación, o las medidas cautelares aplicables. No obstante, el principal problema no solo es procesal, si no que tiene que ver con un tema de cambio de mentalidad de los operadores jurídicos y actores del derecho, ya que la concepción penal actual se sigue centrando solamente en la persona natural como sujeto activo del delito y muy poco en la persona jurídica, ignorando todas las figuras societarias, fusiones, adquisiciones y demás cuestiones que envuelven a la persona jurídica, por lo que debe trabajarse el concepto de derecho penal corporativo. Sobre el impacto del proceso penal a la persona jurídica, este se manifiesta de muchas formas, empezando por el impacto reputacional, especialmente a las empresas que tienen marcas, las cuales pueden verse gravemente afectadas en su valor, y conforme vaya avanzando el caso, a una acusación o juicio, podrá incluso perder libertades económicas y su patrimonio.
Virginia del Pilar Naval Linares	Considera que el Perú no se encuentra preparado para procesar personas jurídicas en general, ello en principio porque los operadores de justicia cuentan con criterios disímiles y existe una falta de consenso en aplicar criterios propios de las consecuencias accesorias.

	Adicionalmente la ley 30424 ha traído la falsa idea de que se tratarían de una responsabilidad administrativa, cuando sería penal, lo cual traerá confusiones en la aplicación correcta del derecho. Por otro lado, destaca el impacto que recae sobre la persona jurídica expuesta el proceso penal, el cual es principalmente de naturaleza civil, como embargos y medidas cautelares, y el impacto reputacional, a pesar de no haber sido condenada, a lo cual se le denomina "la pena del banquillo".
Luis Miguel Reyna Alfaro	Considera que el Perú no está preparado, no solo asociado al tema de los delitos informáticos, si no asociado a dificultades propias de las personas jurídicas, y ello tiene que ver con una percepción de raíces de White Collar Crime, ello porque a ciertos delincuentes no se les considera delincuentes, al existir la idea de que la criminalidad de empresa no es una real criminalidad. Es por eso que, el operador de justicia penal no ha sido capaz de realizar un adecuado tratamiento de la persona jurídica. En el caso de delitos informáticos, este tiene el problema adicional de la técnica, el argumento, y su propia dificultad de investigación. Asimismo, el impacto del proceso penal en la persona jurídica es básicamente operacional y reputacional, que trae como consecuencia las relaciones corporativas, haciendo que muchas veces la persona jurídica se vea expuesta a la denominada "Pena del banquillo", como sucedió con la empresa auditora Arthur Andersen, en el caso Enron.
Fernando Ikehara Veliz	Considera que el Perú no se encuentra preparado para procesar

	penalmente a la persona jurídica por un delito informático o cualquier otro que se encuentre regulado en nuestro ordenamiento jurídico. Esto, en tanto no tenemos un adecuado desarrollo sobre las fórmulas de atribución de responsabilidad, vale decir, una teoría del delito para la persona jurídica. Agrega que, el principal impacto que tiene la persona jurídica cuando es involucrada en un proceso penal, es el tema del daño reputacional. Las empresas no buscan de ser vinculadas con procesos penales, ni siquiera cuando están en posición de agraviados, no quieren tener nada que ver, porque para ellas es un costo alto en la realización de sus actividades, por ejemplo, que sucede cuando una empresa resulta tercer civilmente responsable en un proceso penal que es mediático, lo cual termina teniendo un efecto económico en sus ventas y por ende en ganancias.
Adré Sota Sánchez	Precisa que, nuestra legislación procesal penal es deficiente en cuanto al procesamiento penal de una persona jurídica. Por lo que ve, no existen reglas claras para su incorporación al proceso penal ni para el título de imputación que les corresponde; asimismo, no hay pronunciamientos jurisprudenciales vinculantes sobre la materia, solo vemos el Acuerdo Plenario 7-2009/CJ-116 y un reciente acuerdo plenario de la sala penal nacional. Por otro lado, en cuanto a los operadores del Derecho, ve como positivo que se haya creado una Fiscalía especializada en estos delitos, con sus respectivos despachos fiscales, conociendo que los Fiscales que ocupan

	dichos despachos recibieron especializaciones en la materia, por ende, cree que están preparados para afrontar los retos de dirigir una investigación por delitos informáticos. Asimismo, menciona que la PNP tiene una unidad especializada, no obstante, con grandes limitaciones técnicas y los problemas de corrupción que acechan la institución policial. Agrega que es necesaria la creación de una subespecialidad penal en el Poder Judicial, de jueces especializados en delitos informáticos y defraudaciones a través de las nuevas tecnologías. Sobre el impacto de la persona jurídica en un proceso penal, refiere que consiste en lidiar con la posibilidad de no continuar con su línea de negocio, como lo hacían ex ante a la comisión del delito, también el impacto sobre sus colaboradores y principales ejecutivos, y el impacto reputacional que es una variable importante por considerar, pero es transversal a cualquier tipo de impacto sobre la persona jurídica.
Daniel Ernesto Peña Labrín	No considera que exista un adecuado procesamiento de la persona jurídica, ya que para hacerlo se debería realizar una reforma procesal en el vigente código adjetivo, que bajo el principio de legalidad establezca de manera indubitable las condiciones que salvaguarden el debido proceso y la tutela jurisdiccional efectiva.
Manuel Ibarra Trujillo	Refiere que lo órganos persecutores del delito no se encuentran preparados para investigar estos delitos, por la escases de recursos y la aparente desatención del sistema de justicia para con estos delitos. Por otro lado, menciona

	que la norma penal actual permite que una PJ sea investigada y sancionada aplicando las consecuencias accesorias del delito, no obstante, esta figura ha sido poco utilizada, y sumado a la complejidad de que por si tienen los delitos informáticos, investigar a empresas involucradas con esta normativa sería aún más difícil.
Carlos Quisse Sánchez	Precisa que en la actualidad ni el Ministerio Público se encuentra preparado para investigar delitos informáticos de forma eficiente, y más aún en ambientes empresariales. Por otro lado, refiere que podríamos entender por procesamiento penal, a que la persona jurídica deba ser investigada y procesada en el marco de la ley de responsabilidad administrativa, a lo que sí resultaría adecuado, no obstante, la normativa actual (ley 30424) se encuentra aún en una fase experimental, por lo que, dependiendo de su desarrollo, se abrirá la posibilidad de aumentar su catálogo de delitos.

Análisis documental

Tabla 4

Hallazgo N.° 2

N.° de Expediente	Resultado
N.° Expediente / N.° Resolución 00189-2016-13-5201-jr-pe-04 / res. 3°	De la búsqueda realizada, y el análisis jurisprudencial correspondiente, se advierte que a la fecha no existen procesos a nivel judicial en los cuales se investiguen o procesen a personas jurídicas involucradas en la comisión de delitos informáticos. Por lo que en respuesta al objetivo de que, si existe un adecuado procesamiento de la persona jurídica
N.° Expediente / N.° Resolución 00189-2016-13-5201-jr-pe-04 / res. 2° / auto admisorio	

N.° Expediente / N.° Resolución °189-2016-13-5201-jr-pe-04 / res n.° 8	involucrada en la comisión de delitos informáticos, la practica jurisdiccional y fiscal peruana se ve en la imposibilidad material de dar respuesta, al ser una figura sin casos prácticas y por ende en ausencia de pronunciamientos del sistema penal. No obstante, lo que si existen son pronunciamiento de incorporación de personas jurídicas a procesos penales en aplicación de consecuencias accesorias del delito por delitos económicos y contra la administración pública, como corrupción de funcionarios y lavado de activos. En dicho sentido, estos pronunciamientos determinan el modelo vigente de heteroresponsabilidad vicarial trasladada (Art. 105° del Código Penal), estableciendo lo requisitos generales de procedibilidad para cualquier delito (incluido delitos informáticos), exigiendo una vinculación del delito cometido por la persona natural con la persona jurídica, denominada cadena de atribución, evidenciando así la instrumentalización de la persona jurídica para realizar, encubrir o favorecer un delito informático
N.° Expediente / N.° Resolución N°160-2014-298/ res. °5	
N.° Expediente / N.° Resolución 189-2016-17-5201-jr-pe-04 / res. N.° 3	
N.° Expediente / N.° Resolución Exp. N.° 16-2017-79/ res. N.° 11	
N.° Expediente / N.° Resolución 00016-2017-79-5001-JR-PE-01/ RES. N.° 5	
N.° Expediente / N.° Resolución N°189-2016-14-5201-jr-pe-04 / res. N.° 5	

En relación con el Objetivo Específico 1: Analizar qué elementos de juicio deben valorarse para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos informáticos.

Asimismo, se plantearon las siguientes preguntas en relación con el objetivo específico 1:

- A su criterio, dentro de un proceso penal por delitos informáticos ¿Qué elementos deberían valorarse para incorporar a una persona jurídica involucrada y en base a que elementos se determinaría su eventual responsabilidad?
- A su criterio, en el caso de que los delitos informáticos se incluyan en la Ley 30424, ¿Qué elementos particulares debería tener un programa de prevención para obtener el eximente de responsabilidad por cibercrímenes?

Al respecto se obtuvieron los siguientes resultados:

Entrevista

Tabla 5

Hallazgo N.° 3

Entrevistado	Respuestas
Carlos Dino Caro Coria	Precisa que desde su punto de vista un aspecto importante es la peligrosidad objetiva de la persona jurídica (lo cual debe plantearse como tesis primigenia), no obstante, el Poder Judicial no sostiene dicha postura, y por el contrario a abrazado la posición de la fiscalía donde dice que la peligrosidad objetiva es algo que deberá probarse a lo largo del proceso. No obstante, considera que la peligrosidad objetiva es un elemento clave para la imputación y el derecho de defensa, y al no tener una visión preliminar de este la persona jurídica no puede defenderse a sí misma, y prácticamente tendrá que defender a la persona natural, ya que compartiría su imputación. Sobre el programa de prevención, refiere que, si hablamos de *cibercompliance*, se debe analizar desde los factores de riesgo, dado que la ciberdelincuencia tiene múltiples características, e incluso pueden ser mucho más amplio como el lavado de activos, fraudes colectivos o piramidales cometidos mediante sistemas de blockchain, que, si bien no está en la ley de delitos informáticos, deben ser considerados en el mapa de riesgos de cada organización con un *cibercompliance*. Por otro lado, los elementos o factores esenciales son los establecidos en el reglamento de la ley

	30424, que es el D.S. 002-2019-JUSTICIA, y los lineamientos de la SMV para implementar programas de cumplimiento, e incluso tomar los lineamientos propios de temas generales de *compliance* que son los de la ISO 37301.
Virginia del Pilar Naval Linares	Los elementos que deben valorarse en esta etapa, siempre en grado de prognosis y de ninguna manera certeza, son (i) que el delito se haya cometido por alguna persona natural dependiente de ella o que la represente, (ii) que se haya cometido el ilícito penal en su interés, provecho o beneficio, necesariamente, y (iii) que la persona jurídica haya incumplido sus deberes de dirección, control y supervisión. Estos mismos elementos en grado de certeza deberán concurrir para el establecimiento de la responsabilidad penal. Asimismo, para efectos de aplicar la eximente, debería haberse implementado un modelo de prevención con anterioridad al ilícito penal, que cumpla un estándar alto, como el contenido en la ISO 37301, sistema de gestión de cumplimiento; con especial verificación del cumplimiento de los controles no financieros, tendientes a cautelar el acceso y buen uso de los recursos tecnológicos de la empresa.
Luis Miguel Reyna Alfaro	Considera que independientemente del delito los elementos de incorporación son los mismos, esto es la vinculación de la persona jurídica con el delito. Siendo que, en el caso concreto de delitos informáticos, como el uso de sistemas u otras tecnologías de la empresa encajaría en una instrumentalización de la persona

	jurídica. Con relación al *compliance* se ha popularizado mucho el concepto de elementos de un programa de *compliance*, no obstante, su posición es que se debe trabajar desde un enfoque de riesgos, para realizar una correcta evaluación de riesgos particulares, en el caso concreto basado en seguridad informática, siendo necesario para ello reglamentos de protección de datos, lo que se traduce en una correcta gestión de riesgo empresarial, mediante el uso de un mapa de riesgos.
Fernando Ikehara Veliz	Considera que debe verse que el delito se haya cometido dentro de la actividad económica de la empresa, es decir, la existencia de un factor objetivo que vincule a la empresa con el delito, y el segundo punto consiste en los mecanismos que ha utilizado la persona jurídica para prevenir la comisión de delitos en general, más allá de que sean delitos informáticos. En consecuencia, es necesario que exista un programa de cumplimiento penal, y que este haya sido especialmente diseñado para la actividad económica de la compañía. Sobre el eximente de responsabilidad, precisa que el programa de cumplimiento penal tiene que tener una concepción penal, en dicho sentido, si lo vemos desde una óptica funcionalista, habría que determinar si un programa de cumplimiento penal es un elemento de descarga de imputación objetiva, o una causa de justificación, porque si digo que si es una descarga de imputación objetiva, quiere decir que está dentro del riesgo permitido, dentro de los estándares, por lo que sería el eximente de responsabilidad tanto penal y civil, al ser una conducta estandarizada dentro del riesgo permitido. Caso contrario, si fuera

	una causa de justificación, no podría ser un eximente de responsabilidad, si no un atenuante de la misma, dado que existe una conducta típica bajo el riesgo prohibido.
André Sota Sánchez	Refiere que, para incorporar, a nivel de sospecha inicial simple, deben existir indicios sobre la existencia de un defecto de organización permanente en el tiempo que posibilitó la realización de un delito informático por una persona con poder de representación jurídica o fáctica, en beneficio de la persona jurídica. Para condenar, el estándar es más allá de toda duda razonable. Por ende, debe probarse la existencia de un permanente defecto de organización en cuya permanencia se ejecutó el acto delictivo en beneficio de la persona jurídica. Sobre los elementos del programa de prevención, menciona que no hay ninguno en particular, pues no están pensados en delitos concretos y tampoco deberían regularse de manera expresa a nivel de una resolución administrativa, decreto supremo, ley o decreto legislativo. En concreto, estos riesgos se ven en la política de identificación, evaluación y mitigación de riesgos y, tomando como base la política de *compliance* penal, deberían formularse controles preventivos y/o reactivos frente a los riesgos de delitos informáticos.
Daniel Ernesto Peña Labrín	Dentro de los elementos de valoración, en una adecuada reforma debe considerarse de forma relevante lo siguiente: 1.-Que se constate la comisión de un hecho delictivo por el que la responsabilidad penal de una persona jurídica esté tipificada.

	2.-Que la entidad reciba algún beneficio directo o indirecto por el hecho en sí y que no cuente con las medidas adecuadas para prevenir la comisión de ese delito en concreto (es decir, un Sistema de *Compliance* penal).
Manuel Ibarra Trujillo	Precisa que debe acreditarse con los suficientes elementos, la relación o nexo entre el delito cometido, la persona natural, y la empresa en sí, mediante un nexo lógico que permita inferir que la persona jurídica fue utilizada o instrumentalizada para un fin ilícito, y en el caso concreto de delitos informáticos, que haya utilizado su estructura empresarial o sus recursos tecnológicos para cometer un delito informático. Por otro lado, menciona que la ley 30424 establece los elementos esenciales de un programa de *compliance*, no obstante, estos deben ser adaptados al modelo de prevención de riesgos de delitos informáticos, los cuales tienen una naturaleza técnica.
Carlos Enrique Quisse Sánchez	Refiere que los elementos normativos de incorporación de una persona jurídica al proceso penal se aplican de forma general independientemente del delito investigado, siendo estos la vinculación a la persona jurídica como factor de atribución. Sobre el modelo de imputación penal, este sería la deficiente gestión de riesgos, siendo que en cuyo caso el *compliance* cumpliría una función determinante. Sobre esto último, al ser los delitos informáticos altamente técnicos, un programa de *compliance* de riesgos informáticos debe también ser ostentar características y cualidades técnicas,

	como un oficial de cumplimiento que conozca temas de riesgos informáticos y un equipo técnico que trabaje en conjunto con el árela legal.

Análisis documental

Tabla 6

Hallazgo N.° 4

N.° de Expediente	Resultados
N.° Expediente / N.° Resolución 00189-2016-13-5201-jr-pe-04 / res. 3°	De lo analizado en la presente resolución, el caso versa sobre la presunta comisión de delitos contra la administración pública y lavado de activos en agravio del Estado. En dicho sentido el juez penal ha valorado los siguientes elementos para incorporar a la persona jurídica al proceso penal: *A) Es decir, el delito se habría cometido en el ámbito del ejercicio de la propia actividad de la empresa. B) Los hechos investigados que relacionan a la empresa impugnante, tienen que ver con la utilización de la misma para favorecer los delitos materia de investigación en el ejercicio de su actividad, favorecimiento que en el caso del delito de colusión agravada sería directo. Así incluso se expresa en el requerimiento, con la frase "al existir evidencia que la organización de dicha persona jurídica ha sido empleada para comisión de los delitos.* Esto quiere decir que los criterios judiciales empleados son, primero, que el delito se haya cometido dentro de las estructuras empresariales, es decir en el ejercicio de su actividad económica, como, por ejemplo, una empresa dedica al sector construcción, energía, saneamiento, o informática, y que el delito se haya genera directa o indirectamente con relación a dicha actividad empresarial. En segundo término, que los hechos investigados, estén relacionados a una utilización de la persona jurídica para cometer delitos, esto es utilizar su estructura empresarial y organización para favorecer, realizar o

	encubrir delitos. Actuando en representación de esta, o mediante su logística o recursos. En caso de delitos informáticos, el criterio vendría a ser el mismo, es decir debe acreditarse a modo preliminar que el delito se haya cometido dentro de la actividad económica y empresarial de la persona jurídica de forma directa o indirecta, como sistemas informáticos o tecnología. Asimismo, que existan suficientes indicios que acrediten la instrumentalización o utilización de la persona jurídica, para realizar, favorecer, o encubrir delitos informáticos, sea mediante la utilización de sus sistemas, sus servidores, o la tecnología desarrollada por esta.
N.° Expediente / N.° Resolución 00189-2016-13-5201-jr-pe-04 / res. 2° / auto admisorio	De lo analizado en la presente resolución, se advierte que versa sobre el auto admisorio de un recurso de apelación interpuesto contra la resolución que resolvió declarar fundado el requerimiento fiscal de incorporación de una persona jurídica al proceso penal. Sin embargo, dicho recurso no fue presentado por la representante legal de la persona jurídica o apoderado judicial como indica la norma procesal penal. Si no, que fue presentado por la persona natural sobre quien recae la imputación penal principal (pretensión punitiva), es decir la persona natural con quien comparte la responsabilidad vicarial. Sin embargo, como establece la norma Art. 90, 91, 92, 93 del Código Procesal Penal, la persona jurídica incorporada al proceso mantiene una autonomía procesal de defensa independiente a la persona natural que la instrumentalizo o sobre quien reca la imputación penal de autor. En efecto, la persona jurídica debe presentar sus recursos y consideraciones de forma independiente a la persona natural autora del delito, dado que la norma otorga a la persona jurídica incorporada los mismos derechos que el imputado de acuerdo con su naturaleza. Por lo que la persona natural imputada penalmente, no puede accionar en nombre de la persona jurídica, sino, solo en su propio derecho, de lo contrario nos

	encontraríamos en una causal de falta de legitimidad para obrar.
N.° Expediente / N.° Resolución °189-2016-13-5201-jr-pe-04 / res n.° 8	De lo analizado en la presente resolución, la valoración judicial recayó en el análisis de la narración circunstanciada de los hechos materia de imputación relacionados a la persona jurídica, detallando la cadena de atribución delictiva, que permitió la comisión de delitos dentro de la actividad de la persona jurídica, para facilitar el acuerdo colusorio, dado que el caso bajo análisis es de colusión agravada.
N.° Expediente / N.° Resolución N°160-2014-298/ res. °5	De lo analizado en la presente resolución, se advierte que la valoración judicial recayó en el análisis de la utilización de las cuentas bancarias de la persona jurídica para cometer el acto ilícito, como lo es lavado de activos. De esta forma, el juez penal a valorado que efectivamente existió una instrumentalización de la empresa (uso delictivo), al haberse utilizado sus activos, para realizar asesorías fictas y dar la apariencia de legalidad.
N.° Expediente / N.° Resolución 189-2016-17-5201-jr-pe-04 / res. N.° 3	La resolución analiza la utilización de las cuentas bancarias de una persona jurídica para cometer el delito de lavado de activos. Prima el papel del Ministerio Público en explicar clara y circunstanciadamente la cadena de atribución de la instrumentalización delictiva de la persona jurídica, dentro de su actividad empresarial.
N.° Expediente / N.° Resolución Exp. N.° 16-2017-79/ res. N.° 11	La resolución realiza un análisis exegético de las normas procesales penales, que establecen que la incorporación de la persona jurídica al proceso penal se da antes de la culminación de la investigación preparatoria, a fin de que la persona jurídica puede proponer actos de investigación mediante su representante judiciales, así como ejercer los demás derechos de defensa que le asisten.

N.° Expediente / N.° Resolución 00016-2017-79-5001-JR-PE-01/ RES. N.° 5	La resolución determina que, para la incorporación de la persona jurídica al proceso penal, solo deben cumplirse los aspectos formales esenciales que exige la norma procesal. Esto es que se individualice correctamente a la persona jurídica, y que el Ministerio Púbico explique a manera circunstanciada (mas no detallada o específica) la cadena de atribución con la persona jurídicas, es decir su presunta instrumentalización delictiva, no siendo necesaria la sustentación de la peligrosidad objetiva o defecto de organización, lo cual se evaluaría en la etapa de juzgamiento.
N.° Expediente / N.° Resolución N°189-2016-14-5201-jr-pe-04 / res. N.° 5	La resolución precisa que, para la correcta incorporación al proceso penal, debe acreditarse preliminarmente la conexión entre la persona jurídica requerida y las acciones presuntamente ilícitas bajo investigación, dicha conexión recibirá la denominación de cadena de atribución, la misma que deberá ser clara, coherente y circunstancia, al menos a un nivel formal de procedimentalidad. También precisa que en el acto de incorporación no se valoran aspectos sustanciales, como la peligrosidad objetiva, dado que ello corresponderá en la etapa de juicio, donde se realizará la evaluación y procedencia de una consecuencia accesoria, o su negativa.

En relación con el Objetivo Específico 2: Proponer la fórmula de procesamiento penal adecuada para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos.

Asimismo, se plantearon las siguientes preguntas en relación con el objetivo específico 2:

- A su criterio, ¿Considera que debe mantenerse una coexistencia de modelos de procesamiento penal de personas jurídicas, en referencia a la Ley 30424 y el artículo 105 del Código Penal, o por el contrario considera que este último debe ser derogado?

- A su criterio, considerando a los recursos y tecnología que puede ostentar una empresa, ¿Considera que la gravosidad y afectación de un delito informático cometido por una persona jurídica es superior al que cometería una persona natural?
- ¿Considera que los delitos informáticos deben ser considerados en el marco de la Ley 30424?

Al respecto se obtuvieron los siguientes resultados:

Entrevista

Tabla 7

Hallazgo N.° 5

Entrevistado	Respuestas
Carlos Dino Caro Coria	Considera que las consecuencias accesorias (art. 105 C.P.) deben ser derogadas ante su fracaso de más de 30 años de vigencia sin eficacia, y que debe existir un solo sistema de responsabilidad penal de la persona jurídica, mediante un sistema de catálogo abierto de delitos en la Ley 34424, porque todo delito del Código Penal puede ser cometido por la persona jurídica. Asimismo, considera que el nivel de gravosidad que puede generar un colectivo teniendo en cuenta los recursos y la distribución de funciones puede ser mucho mayor en las diferentes etapas del delito.
Virginia del Pilar Naval Linares	Considera que ante la promulgación de la Ley N.º 30424, cierta normativa que puede lugar a contraposiciones o interpretaciones erróneas, deben ser reformadas. El

	artículo 105, si bien no tiene naturaleza de consecuencias penales del delito, propiamente dichas, se concibió cuando aún no se pensaba en que la persona jurídica podría responder de modo autónomo y desligada de la responsabilidad penal de la persona natural. Asimismo, no necesariamente el delito informático por la persona jurídica será siempre más gravoso, no obstante, si será así en los casos de grandes empresas con gran alcance tecnológico, Para finalizar agrega que los delitos informáticos si debiesen ser parte de la ley 30424, pero que su aplicación debe ser muy estricta, verificándose con especial incidencia el beneficio ilícito obtenido por la persona jurídica.
Luis Miguel Reyna Alfaro	Sobre las consecuencias accesorias (art. 105° C.P.) y la responsabilidad autónoma (Ley 30424), que ambos modelos de imputación deben mantenerse, ya que fueron pensados para situaciones diferentes, y tienen una naturaleza distinta, siendo que, en el caso de las consecuencias accesorias del delito, estas tienen como naturaleza jurídica la peligrosidad objetiva de la persona jurídica, y en el caso de la ley 30424, la naturaleza jurídica es el defecto de organización o deficiente gestión de riesgos, por lo que ambos deben continuar. Sobre la gravosidad, depende del resultado, ya que también puede ser el mismo, porque pueden existir personas naturales con tanta capacidad técnica como una persona jurídica, estando la diferencia en el desvalor de la acción. Es posible que una persona jurídica con sus recursos pueda cometer un delito con un efecto multiplicador, pero en caso de

	delitos informáticos no es una regla. Finaliza mencionando que los delitos informáticos deben estar amparados en la Ley 30424 pero no antes de otros delitos como los delitos ambientales o tributarios, que son más identificatorios a la criminalidad empresarial, dado que los delitos informáticos no son exactamente los cometidos por una empresa, sino incluso estarían más asociados al crimen organizado. En dicho sentido hay delitos que tienen una actividad más empresarial que otros.
Fernando Ikehara Veliz	Considera que las consecuencias accesorias deben ser derogadas, y todo debe ir a la Ley 30424, siendo que ha permitido traer sobre la mesa el debate sobre la responsabilidad autónoma de la persona jurídica, y la necesidad de una teoría del delito para esta, así como ver a la persona con una perspectiva funcionalista que identifica a la persona como único sujeto de imputación independientemente de que sea persona natural o jurídica. Asimismo, que crea el incentivo para la PJ al tener el programa de prevención, lo cual tendría aspectos positivos, como la disminución de actividades ilícitas en ambientes empresariales, y el apoyo de control que tendrá el Estado en la propia empresa. Sobre la gravosidad del delito informático cometido por una PJ menciona que es discutible, porque no toda persona jurídica está en una posición superior para cometer estos delitos, o que tiene mayores recursos, lo cual no siempre es cierto.
André Sota Sánchez	Sobre la Ley 30424 y el artículo 105 del Código Penal (consecuencias accesorias), refiere que decidirse por uno

	de ellos, no pueden coexistir pues llegamos a casos confusos. No tiene sentido derogar el art. 105, pues puedes leer e interpretar el mismo en clave del art. 3° de la Ley N.° 30424 y sigue siendo lo mismo. En concreto, debería incorporarse al Código penal el régimen de responsabilidad penal de las personas jurídicas. Sobre la inclusión de los delitos informáticos en la ley 30424, menciona no estar de acuerdo porque usualmente son las personas jurídicas las afectadas por estos delitos, no obstante, podrían incluirse determinados delitos que son cometidos a favorecimiento de la P.J.
Daniel Ernesto Peña Labrín	Considera que deben coexistir los modelos de imputación de la persona jurídica (Ley 30424 y consecuencias accesorias Art. 105 CP), siendo que, bajo el principio de legalidad se debe implementar la reforma de su convivencia. En dicho sentido las medidas accesorias deberían llevarse a un modelo mixto en la procura de aprovechar sus bondades y fortalecer la reforma procesal. Sobre la gravosidad de los delitos informáticos cometidos por una persona jurídica, considera que, en base a su economía y tecnología, su accionar delictivo podría alcanzar niveles insospechados. Sobre la inclusión de los delitos informáticos en la ley 30424, refiere estar de acuerdo, ya que la modalidad "números clausus" que preconiza la citada ley, ya fue superada por la realidad y es tiempo que la norma aludida sea actualizada a las nuevas modalidades de criminalidad no convencional y así darles a los órganos formales del control de la criminalidad, las herramientas típicas y procesales

	adecuadas a los nuevos fenómenos delictógenos informáticos del siglo XXI. Urgiendo la reforma procesal en dichos términos.
Manuel Ibarra Trujillo	Considera que dependiendo del desarrollo de la ley 30424, se podrá hablar de la derogación de las consecuencias accesorias, siendo que ambas son se casi reciente aplicación en la práctica. No obstante, en un futuro el modelo de imputación deberá inclinarse a la ley 30424. Ello porque el nivel de afectación de un delito cometido por una persona jurídica siempre será mayor, por los recursos que posee, tanto económicos como tecnológicos, pudiendo afectar a miles o a millones de personas cuando hablamos de delitos informáticos, que fueran cometidos por ejemplo por una empresa de telecomunicaciones. Agrega que expandir los delitos informáticos dentro de la ley 30424 ayudaría a la persecución de una persona jurídica involucrada, pero es algo que la practica forense determinará con la aplicación de la normativa.
Carlos Enrique Quisse Sánchez	Menciona que preliminarmente, deben mantenerse en nuestro ordenamiento tanto las consecuencias accesorias a la PJ y la responsabilidad administrativa de la PJ, hasta que el catálogo de delitos de esta última se expanda, en cuyo caso cuando suceda, podría ser posible la derogación de las consecuencias accesorias, no obstante, previo trabajo de análisis si estas aún tienen sentido para determinados delitos por su naturaleza o baja afectación. Por otro lado, afirma que, debido a sus recursos, medios y organización, el

	delito informático cometido por una persona jurídica puede tener un nivel de afectación mucho mayor. Finaliza que los delitos informáticos, por un sentido de merecimiento de pena si debieran ser considerados en la ley 30424, no obstante, al estar aún en una etapa de experimentación de la norma, esto deberá hacerse más adelante.

Análisis documental

Tabla 8

Hallazgo N.° 6

N.° de Expediente	Resultado
N.° Expediente / N.° Resolución 00189-2016-13-5201-jr-pe-04 / res. 3°	De la búsqueda y análisis jurisprudencial, y como ha sido previamente advertido, no existen a la fecha procesos penales contra empresas por la comisión de delitos informáticos en el Perú, siendo que los que se encuentran en transcurso son por delit0s económicos y contra la administración pública, por lo que en la práctica jurisdiccional nacional existe una ausencia de casos, por lo que la jurisprudencia de procesos penales contra personas jurídicas se encuentran en la imposibilidad material de responder el objetivo de investigación de proponer una fórmula de procesamiento penal adecuado para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos, siendo que en el modelo de imputación vigente (consecuencias accesorias) no se ha llevado a la práctica ningún caso.
N.° Expediente / N.° Resolución 00189-2016-13-5201-jr-pe-04 / res. 2° / auto admisorio	
N.° Expediente / N.° Resolución °189-2016-13-5201-jr-pe-04 / res n.° 8	
N.° Expediente / N.° Resolución N°160-2014-298/ res. °5	
N.° Expediente / N.° Resolución 189-2016-17-5201-jr-pe-04 / res. N.° 3	
N.° Expediente / N.° Resolución Exp. N.° 16-2017-79/ res. N.° 11	
N.° Expediente / N.° Resolución 00016-2017-79-5001-JR-PE-01/ RES. N.° 5	

N.° Expediente / N.° Resolución N°189-2016-14-5201-jr-pe-04 / res. N.° 5

CAPÍTULO IV: DISCUSIÓN Y CONCLUSIONES

El presente trabajo ha tenido como finalidad brindar a la comunidad jurídica y los operadores de justicia una aproximación al procesamiento penal de la persona jurídica involucrada en la comisión de delitos informáticos, siendo esta una de las primeras investigaciones en aproximarse al fenómeno del ente colectivo ciberdelincuente. Ello a la luz del amplio desarrollo tanto empresarial y tecnológico de los últimos años, lo que deviene en necesario que los operadores jurídicos tengan conocimiento de las formas de procesamiento penal contra entes colectivos, al estar dentro de sus riesgos la posibilidad de un cibercrimen.

Ahora bien, la presente investigación ha seguido una estructura académica estandarizada, exponiendo el correspondiente marco teórico aplicable, recabando las investigaciones previas (aunque no exactas del tema al ser una investigación exploratoria), y aplicando los respectivos criterios metodológicos e instrumentos de investigación, siendo estos últimos la guía de análisis documental y la entrevista a expertos, recabando valiosa información a fin de dar respuesta a las problemáticas planteadas.

4.1. Limitaciones

No obstante, es necesario resaltar que parte de los límites de la investigación fue que en el Perú no existen antecedentes en los que se haya procesado penalmente a una persona jurídica por estar involucrada en la comisión de delitos informáticos, situación que también parece compartir el resto del mundo, siendo que en el Perú, los casos en los cuales se ha procesado penalmente a una persona jurídica, ha sido por la comisión de delitos contra la administración pública, relacionado a casos de corrupción y lavado de activos (Caso Odebrecht), en aplicación del artículo 105° del Código Penal (consecuencias accesorias del

delito) en etapa incorporación al proceso. Por lo que, a la fecha, no han existido pronunciamientos judiciales sobre la responsabilidad de alguna persona jurídica por delitos informáticos, por lo que la guía de análisis documental de resoluciones judiciales, se basó específicamente en los criterios de incorporación procesal de la persona jurídica, excluyendo del análisis lo referido a los delitos imputados, para luego en el capítulo de discusión, interpretar la posible aplicación de dichos criterios generales de incorporación a imputaciones por delitos informáticos. Al respecto, otra limitación fue la ausencia de especialistas de la materia de Derecho Penal de la Empresa, por lo que existieron demoras y retrasos en recabar la información de las entrevistas a expertos.

En dicho sentido, cabe mencionar que no existen antecedentes de investigación al tema específico bajo estudio, por lo que se recopilaron antecedentes de investigaciones aproximadas al tema, en consecuencia, la presente investigación tiene carácter exploratorio. Del mismo modo, al ser un tema especializado se tuvo que considerar antecedentes de investigación con un espacio temporal más alto, al considerarse que eran investigaciones que se relacionaban sustancialmente a la investigación.

4.2. Discusión

Ahora bien, se pasará a exponer los tópicos de discusión, como acuerdos, desacuerdos e interpretación de los resultados, antecedentes y marco teórico, en base a los objetivos de investigación que han guiado el presente trabajo, cabiendo precisar que la presente investigación es de enfoque cualitativo y exploratoria, sin hipótesis sujeta a comprobación, por lo que no busca aportar al conocimiento jurídico del objeto de investigación

4.2.1. Objetivo general

Determinar si existe un procesamiento penal adecuado de la persona jurídica involucrada a la comisión de delitos informáticos en el Perú al año 2022.

En este punto, de los resultados de la entrevista, tal y como expusieron Sota (2022), Ibarra (2022), Quisse (2022), existen dos enfoques cuando hablamos de procesamiento penal de personas jurídicas involucradas en delitos informáticos. El primer enfoque abarca el sentido procesal material, es decir en las facultades y recursos de investigación que tienen los órganos persecutores del delito, como lo son el Ministerio Público y la Policía Nacional. En dicho sentido los entrevistados coinciden en que las citadas instituciones carecen de los recursos técnicos, humanos y organizativos para investigar y procesar delitos informáticos de forma satisfactoria, sumando a ello la complejidad de que dicho delito se cometa al interior de una estructura empresarial. En dicho sentido es necesario una mayor inversión de recursos públicos destinados a equipar a los órganos persecutores con los elementos necesarios para combatir la ciberdelincuencia, con una policía debidamente preparada con el personal suficiente especializado en investigación de delitos cibernéticos, asimismo, hacen falta fiscales con una preparación especializada en Derecho Penal Informático, no obstante como refirió Sota, la creación de las Fiscalías Especializadas en Ciberdelincuencia representan un gran avance en la investigación de estos delitos.

El otro enfoque del procesamiento penal de personas jurídicas involucradas en delitos informáticos, es el que se encarga de analizar las estructuras procesales propiamente dichas dentro del proceso penal común (investigación preparatoria, etapa intermedia, y juicio), en dicho sentido, el marco jurídico vigente, es que una persona jurídica que se vea involucrada en la comisión de delitos informáticos, sea porque fuera utilizada para favorecer, encubrir o realizar el delito, siempre y cuando la persona natural que cometió el delito sea identificada e individualizada, podrá ser incorporada al proceso penal en aplicación de las consecuencias accesorias del delito reguladas en el Art. 105 del Código Penal, en dicho sentido, Caro (2022) en concordancia con Sota (2022), precisó que uno de los principales problemas de esta fórmula de imputación, es que la legislación es general e incipiente, teniendo grandes falencias en los principios y garantías procesales que le debieran asistir a la persona jurídica, como la imputación concreta o la no autoincriminación, y que dichas falencias no solo emanan de una deficiente legislación, sino también de una mentalidad imperante en el

sistema de justicia peruano (fiscal y jurisdiccional), donde se está acostumbrado a ver como sujeto pasible de derecho penal a la persona humana solamente, no comprendiéndose el concepto de Derecho Penal de la Empresa, que tiene reglas y principios de imputación específicos, por lo que se debe construir una nueva mentalidad de Derecho Penal Corporativo.

Asimismo, Naval (2022) también refiere que existe una ausencia de criterios uniformes en relación con las consecuencias accesorias, en parte por su escasa aplicación a lo largo de los años. Añade que la Ley 30424 viene generando confusiones, al tener la etiqueta de responsabilidad "administrativa", cuando en realidad trata de una verdadera responsabilidad penal de la persona jurídica, siento este mismo criterio compartido por Caro.

Por su lado, Reyna (2022) concuerda en que existe una errónea percepción de los delitos empresariales por parte del sistema de justicia penal, la que toma a la criminalidad empresarial como una no verdadera criminalidad, siendo por eso que el operador de justicia penal no es capaz de realizar un adecuado tratamiento de la persona jurídica, agrando que en el caso concreto de los delitos informáticos, se suma la complicación de la técnica y el argumento de imputación, propias de la naturaleza de estos delitos, lo cual aumenta la problemática del asunto. En relación con los antecedentes de investigación, Navas y Jaar (2018), desde la óptica de la legislación chilena, mencionaba que aún la jurisprudencia no venía aplicando correctamente los presupuestos de la responsabilidad penal de la persona jurídica, siendo que aún existían problemas de fundamentación sobre la real dirección o supervisión que ejercía la persona natural imputada sobre la empresa, y la acreditación de que dicho ilícito fuera en beneficio directo de la persona jurídica, lo cual a criterio del autor quedaba como un vacío de la práctica judicial.

Ahora bien, si bien es cierto, los entrevistados concuerdan tal y como quedó en el marco teórico, que, de acuerdo con la normativa vigente, el procesamiento penal por delitos informáticos contra una persona jurídica se daría en aplicación de las consecuencias accesorias (artículo 105° del Código Penal), cuando hablamos de Procesamiento Penal de Personas Jurídicas, esto abriría a otros conceptos también relacionados como el de Responsabilidad Penal de la Persona Jurídica. Con relación a lo anterior Ikehara (2022), mencionó que no se puede hablar propiamente de un Derecho Procesal Penal de La Persona Jurídica, hasta que no quede claro un Derecho Penal de la Persona Jurídica, lo que se traduce

en la ideación de una correcta teoría del delito aplicable a las personas jurídicas, siendo que esto último se ha convertido en el esfuerzo conjunto de los dogmáticos de los últimos tiempos. Dicha posición concuerda con la expuesta por García (2012), en su artículo de investigación titulado "Esbozo de un modelo de atribución de responsabilidad penal de las personas jurídicas", donde destacó lo insuficiente de un modelo de imputación de la persona jurídica limitado a las consecuencias accesorias, siendo necesaria trabajar en una fórmula de imputación penal autónoma. No obstante, Mayer y Oliver (2020), mencionaban que los delitos informáticos deben adaptarse a la teoría del delito convencional, lo que nos lleva a pensar que quizá, en vez de buscar nuevas teorías del delito para la persona jurídica, sería solo necesario buscar el fundamento de adaptación de su imputación a la teoría del delito ya existente.

4.2.2. Objetivo específico 1

Analizar qué elementos de juicio deben valorarse para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos informáticos.

En este punto, Caro (2022) precisa que desde su punto de vista un aspecto importante para valorar, si hablamos de consecuencias accesorias, es la determinación de la peligrosidad objetiva a modo preliminar en el requerimiento de incorporación de la persona jurídica al proceso penal, ello a fin de tener clara una imputación concreta, y las debidas garantías de atribución de responsabilidad del proceso penal, de lo contrario ante la ausencia de postura preliminar de peligrosidad objetiva que constituye la naturaleza jurídica de las consecuencias accesorias, se carece de una imputación concreta de la cual se pueda defender la persona jurídica (desvirtuando la peligrosidad objetiva), y teniendo que desvirtuar las imputación a la persona natural para defenderse a sí misma, lo cual desvirtúa el sentido de la defensa independiente de la persona jurídica. No obstante, dicha posición no ha sido de recibo por la judicatura, la cual, por el contrario, ha aceptado la postura de la Fiscalía, en la cual solo sería necesario acreditar la vinculación entre la persona jurídica, la persona natural imputada y el delito, es decir la denominada cadena de atribución a modo preliminar. Ello ha sido corroborado con el análisis documental realizado sobre la jurisprudencia especializada.

En dicho sentido, según Naval (2022), dicha vinculación consiste en (i) que el delito se haya cometido por alguna persona natural dependiente de ella o que la represente, (ii) que

se haya cometido el ilícito penal en su interés, provecho o beneficio, y (iii) que la persona jurídica haya incumplido sus deberes de dirección, control y supervisión. Al respecto Sota (2022) refiere que para incorporar a nivel de sospecha inicial simple es necesario la existencia de indicios de un defecto de organización permanente en el tiempo. Dicha sospecha, se acuerdo con Ibarra (2022), cosiste Enel nexo lógico entre la persona jurídico y el delito cometido por el dependiente en nombre de la persona jurídica, siendo en el caso de delitos informáticos, que, por ejemplo, la persona natural dependiente, administrador o representante haya utilizado para fines delictivos la estructura empresarial, recursos tecnológicos o data de la persona jurídica.

En referencia al programa de prevención, Caro (2022), Naval (2022), y Sota (2022), coinciden en que para tener un eximente de responsabilidad, deben aplicarse correctamente los elementos esenciales para los programas de cumplimiento, toda vez que fueron pensadas para todo tiempo de riesgo penal. Dichos elementos se encuentran establecidos en el reglamento de la Ley 34424, el Decreto Supremo 002-2019-JUSTICIA, y los lineamientos de la SMV para la implementación de programas de cumplimiento. Así también debe considerarse el lineamiento internacional para todo programa de cumplimiento, el ISO 37301. Por su lado, Quisse (2022), precisa que, al ser los delitos informáticos altamente técnicos, un programa de prevención de riesgos informáticos debe ostentar del mismo modo características técnicas, como un oficial de cumplimiento con conocimiento en ciberseguridad, y un equipo técnico que trabaje de la mano en el área legal. Lo anterior se relaciona con lo expuesto por Blozziers (2018), en sus tesis de maestría titulada “El delito informático y su incidencia en la empresa bancaria”, que manifestada que la afectación de los delitos informáticos a las empresas genera una afectación relevante en términos económicos, lo cual en una interpretación transversal no solo sucedería cuando una empresa es víctima de delitos informático, si no también cuando es procesada penalmente por verse inmersa en su comisión, lo cual recae en el denominado daño reputacional.

Por otro lado, del análisis documental realizado sobre la totalidad de la muestra jurisprudencial estudiada, el razonamiento recae sobre indicios plausibles de la instrumentalización de la persona jurídica, es decir, los pronunciamientos judiciales no

exigen que se acredite de forma certera o cercana, la instrumentalización criminal de la persona jurídica para cometer, encubrir o facilitar el delito, ni tampoco que el Ministerio Público propugne una tesis de peligrosidad objetiva a modo preliminar, si no, que los requisitos probatorios se relajan, por el mismo hecho de estar aún en una etapa de investigación. Exigiéndosele al Ministerio Publico, que solo acredite modo preliminar y mediante indicios, una alta posibilidad de instrumentalización de la persona jurídica, a fin de que dicha instrumentalización o no se termine de acreditar o debilitar en juicio.

Ahora, aplicando dicho criterio de valoración judicial para la incorporación de la persona jurídica por una comisión de delitos informáticos, dependerá de que delito informático se pretende analizar, pero en términos generales, se exigiría que, en el caso de una empresa de telecomunicaciones o tecnologías de la información, un sujeto parte de la organización, utilice las infraestructuras, tecnología y órganos de la empresa, para que esta, en un eventual proceso penal contra el sujeto físico, sea incorporada al proceso, dado que esta instrumentalización criminal la convertiría en un aparente sujeto peligroso, es decir una entidad que genera peligro en la sociedad.

Explicamos nuestra interpretación en el siguiente mapa de creación propia:

Figura 1. Mapa de elementos de incorporación de la persona jurídica al proceso penal.

Ahora bien, cabe precisar que de los resultados comparativos de los antecedes, y tal como lo explicó Blanco (2009), los programas de *compliance* suponen un gasto adicional para la persona jurídica en la prestación de sus servicios, dado que implica gastos de asesoría, consultoría, reforzamiento de controles y elaboración de mapas de riesgo y controles específicos. Siendo que en el caso de empresas de actividad informática, sería necesario invertir en dichos mecanismos de prevención, como sistemas blockchain, hackeo blanco en prevención de vulneraciones de ciberseguridad, elaboración de protocolos y manuales de tratamiento de datos personales, y el fortalecimiento y desarrollo de tecnología que propicie la mitigación de riesgos virtuales, todo a fin de salvaguardar la ciberseguridad de sus clientes o usuarios, así como resguardar los activos de la empresa, lo que a corto plazo devendrá en un gasto cada vez más necesario, y en ocasiones obligatorio para las empresas del rubro informático.

En dicho contexto, en relación al *compliance* de prevención de riesgos penales, Rayon Ballesteros (2018) menciona que es necesario evaluar los riesgos específicos de la empresa, la misma que deberá mitigar los riesgos penales a los cuales se encuentra expuesto de acuerdo con su actividad empresarial. Ello en concordancia con Caro (2020), en su artículo denominado "Imputación objetiva y *compliance* penal", resalta la importancia de una debida diligencia (due diligence) del empresario o miembro del órgano de administración, para que se considere el eximente de responsabilidad penal/administrativa de la persona jurídica, y que, en efecto, dicha debida diligencia se manifiesta en la implementación de un programa de *compliance* o de prevención del delito, que sea eficiente y eficaz, con una aplicación material en la cultura corporativa de la persona jurídica, es decir un control efectivo de las medidas de mitigación de riesgo.

Un aspecto interesante, sujeto a debate, y que puede que la jurisprudencia nunca llegue a responder, es que si un modelo de prevención podría constituir un eximente de responsabilidad en las consecuencias accesorias, dado que la norma penal y procesal penal no lo regula de dicha manera, sin embargo, de acuerdo a la naturaleza jurídica de las consecuencias accesorias, esta recae sobre la peligrosidad objetiva que representa, es decir, al ser instrumentalizada para fines delictivos, sea para realizar, encubrir o facilitar el delito, pasa a generar un riesgo prohibido en la sociedad al tener una deficiente gestión de riesgos y convertirse en un instrumento delictivo, lo cual al considerar que la persona jurídica tiene garantizado su derecho de defensa, deja la puerta abierta a que se pueda debatir en juicio la existencia o no de un programa de prevención con la intención de desvirtuar la peligrosidad objetiva.

4.2.3. Objetivo específico 2

Proponer la fórmula de procesamiento penal adecuada para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos

En este punto, es importante entrar a detallar la discusión sobre la pertinencia o no de la existencia de dos modelos de procesamiento distintos para la persona jurídica en el proceso penal, esto en referencia a las consecuencias accesorias reguladas en el artículo 105° del Código Penal, y la responsabilidad administrativa (penal) de la persona jurídica, regulado en la Ley 30424. Al respecto, Caro (2022), es de la opinión que el artículo 105° debe ser derogado, y la responsabilidad (penal) administrativa o autónoma sea la regla para la persona jurídica. De la misma opinión es Peña (2022), Ibarra (2022), e Ikehara (2022), que mencionan que las consecuencias accesorias han demostrado ser ineficientes, y que

dicha formula de imputación ha sido superada, debiendo reformarse la Ley 30424 de un catálogo *numerus clausus* de delitos, a uno de catálogo abierto, siendo de aplicación ante todos los delitos del Código Penal. No obstante, de opinión contraria es Reyna (2022), el cual precisa que debe mantenerse la coexistencia de modelos de procesamiento, ya que tendrían naturalezas jurídicas distintas, siendo que la naturaleza jurídica de las consecuencias accesorias es la peligrosidad objetiva, en cambio, la responsabilidad administrativa de la persona jurídica tiene como naturaleza jurídica el defecto de organización, o deficiente gestión de riesgos, o también llamado el no *compliance*, por lo que, a criterio de Reyna, al ser de naturalezas jurídicas diferentes, las consecuencias accesorias deben ser derogadas, del mismo criterio es Sota (2022), Naval (2022), y Quisse (2022), no obstante, estos agregan que las consecuencias accesorias debe ser reformadas, subsanando los vacíos legales de aplicación, y estableciendo criterios claros, adicionalmente, manifiestan que también están de acuerdo con que los delitos informáticos se contemplen en la Ley 30424, por un sentido de merecimiento de pena y eficiencia procesal, con la reserva de Sota que agrega que deben ser contemplados solo los delitos informáticos que materialmente tengan tendencia de comisión empresarial, y de Reyna, que es de opinión que también existen otros delitos de mayor naturaleza de comisión empresarial como los delitos tributarios y ambientales.

Implicancias

El presente trabajo de investigación se constituye como la primera investigación en el Perú que tiene como objeto de investigación a la persona jurídica involucrada como sujeto activo en la comisión de delitos informáticos y su procesamiento penal a la luz del Nuevo Código Procesal Penal del 2004, por lo que los resultados tienen implicancias tanto prácticas, académicas y de *lege ferenda*. Sobre la primera, brindará las bases teóricas y el conocimiento jurídico necesario para que los operadores jurídicos puedan procesar penalmente a empresas

(o personas jurídicas en general) que hayan sido instrumentalizadas para realizar, facilitar o encubrir un hecho ilícito, siendo esta una figura de casi nula aplicación en la práctica judicial peruana (consecuencias accesorias aplicables a la persona jurídica), y que merita mayor desarrollo doctrinal e investigativo. Sobre las implicancias académicas, al ser una primera aproximación investigativa al fenómeno de la *empresa ciberdelincuente*, servirá de base a mayores estudios en el futuro, ello en consideración de los casos que se presenten en la praxis judicial, lo cual consideramos será en el futuro próximo. En relación a la tercera implicancia de *lege ferenda,* servirá de fundamento doctrinario y científico al legislador para la discusión de modificación de la Ley 30424 Ley que regula la responsabilidad administrativa de la persona jurídica, a fin de que los delitos informáticos sean incluidos en su catálogo de delitos, ello considerando que el Proyecto de Ley 5630/2020-CR Ley de seguridad informática y represión de los delitos informáticos se encuentra en comisión pendiente dictamen. Dicho todo lo anterior, se evidencia la plena utilidad del presente trabajo.

4.3. Conclusiones

Podemos concluir que en el Perú no existe un adecuado procesamiento penal de la persona jurídica involucrada en la comisión de delitos informáticos, lo cual se divide en dos aspectos, el primero de ellos es el aspecto procesal propiamente dicho, siendo que de acuerdo al modelo vigente, sería de aplicación las consecuencias accesorias aplicables a la persona jurídica reguladas en el artículo 105° del Código Penal, también denominada responsabilidad trasladada, vicarial, o heteroresponsabilidad, no obstante dicha formula de imputación ha tenido una escasa aplicación en nuestro ordenamiento jurídico, y aún mantiene deficiencias normativas y de aplicación práctica, siendo uno de los principales problemas la resistencia por parte de los operadores del sistema de justicia penal a la comprensión del Derecho Penal Corporativo o Derecho Penal de la Persona Jurídica o Empresa, la cual tiene reglas de

imputación, y garantías y principios procesales, como el de imputación concreta, no autoincriminación, entre otros. El segundo aspecto, del deficiente procesamiento de personas jurídicas involucradas en la comisión de delitos informáticos, es referente a la actuación material de los órganos persecutores del delito, siendo estos la Fiscalía y la Policía Nacional, los cuales, si bien han tenido avances en la investigación de ciberdelitos, aún se encuentran en proceso de adaptación y mejora en la materia.

En referencia a que elementos de juicio deben valorarse para incorporar y procesar penalmente a una persona jurídica involucrada en la comisión de delitos informáticos, dentro de las consecuencias accesorias, independientemente del delito la jurisprudencia ha resuelto que es necesaria la vinculación entre la persona jurídica, persona natural vinculada, y el delito que se hubiera cometido, recibiendo el nombre de cadena de atribución. No obstante parte de la doctrina, mantiene como posición que también debe considerarse la fundamentación preliminar de la peligrosidad objetiva de la persona jurídica, toda vez que su naturaleza jurídica consiste en dicha peligrosidad, al mismo tiempo que obedecería a un principio de imputación necesaria. Sobre el programa de prevención y el eximente de responsabilidad, para un correcto programa de prevención deben cumplirse los elementos esenciales de los programas de cumplimiento, al ser aplicables para todo tipo de delito. Dichos elementos se encuentran establecidos en el reglamento de la Ley 34424, Decreto Supremo 002-2019-JUSTICIA, y los lineamientos de la SMV para la implementación de programas de cumplimiento. También debe considerarse el lineamiento internacional para todo programa de cumplimiento, el ISO 37301.

Asimismo, se concluye que para procesar adecuadamente a una persona jurídica involucrada en la comisión de delitos informáticos es pertinente que se incluyan los delitos informáticos en el catálogo de delitos de la Ley 30424 “Ley que regula la responsabilidad administrativa de las personas jurídicas” a fin de que dichas empresas sean procesadas de forma autónoma, por lo que el Proyecto de Ley 5630/2020-CR Ley de seguridad informática y represión de los delitos informáticos, es viable estando de conformidad con los principios de eficacia y eficiencia procesal.

REFERENCIAS

Abad, G. (2019). El Criminal Compliance: la Responsabilidad Penal de las. *ADVOCATUS*, 111-120.

Agencia EFE. (2020). *Ciberseguridad: en el 2020 van 15 denuncias contra empresas en el Perú*. Gestión: https://gestion.pe/peru/ciberseguridad-en-el-2020-van-15-denuncias-contra-empresas-en-el-peru-noticia/?ref=gesr

Alfonso, I. (2016). La Sociedad de la Información, sociedad del conocimiento, y sociedad del aprendizaje. *Bibliotecas anuales de investigación*, 235-243.

Allievi, M. (2022). *Nueve de cada diez empresas españolas sufrió al menos un ciberataque en 2021*. El País: https://elpais.com/economia/2022-02-10/nueve-de-cada-diez-empresas-espanolas-sufrio-al-menos-un-ciberataque-en-2021.html

Altuna, M. d. (2018). *Guía de investigación científica 2018.* Lima: Universidad Privda del Norte.

Alvarez Risco, A. (2020). *Clasificación de las Investigaciones.* Universidad de Lima. https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/10818/Nota%20Acad%c3%a9mica%202%20%2818.04.2021%29%20-%20Clasificaci%c3%b3n%20de%20Investigaciones.pdf?sequence=4&isAllowed=y

BBC Mundo. (2018). *5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día*. BBC NEWS: https://www.bbc.com/mundo/noticias-43472797

Beck, U. (2002). *La sociedad de riesgo.* Barcelona: Paidós.

Blossiers, J. (2018). El delito informático y su incidencia en la empresa bancaria. *Tesis de maestria*. Universidad Nacional Federico Villareal: Lima.

Boletín de Prensa. (2021). *EY Perú: más del 60% de empresas peruanas muestra preocupación por su capacidad para enfrentar ataques de ciberseguridad*. EY Building a better working world: https://www.ey.com/es_pe/news/2021/10/empresas-peruanas-preocupacion-ataques-ciberseguridad

Canet, F. (2016). Cibercriminalidad: especial referencia al delito de usurpación y suplantación de identidad. *Tesis de maestria*. Universidad Internacional de La Rioja: Valencia.

Cárdenas-Solano, L., & otros, y. (2016). Gestión de seguridad de la: Información: revisión bibliográfica. *El profesional de la información*, 931-948.

Caro, C. (2020). Imputación objetiva y compliance penal. En E. Demetrio, *Derecho Penal Económico y Teoría del Delito* (págs. 371-409). Valencia: Tirant Lo Blanch.

Caro, C., & Reyna, L. (2019). *Derecho Penal Económico y de la Empresa.* Gaceta Jurídica.

Carrillo, C., & Montenegro, A. (2018). La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos. *Tesis de grado*. Universidad Señor de Sipan: Pimentel.

CEGESTI. (2006). *Manual para la implementación de la responsabilidad social empresarial.* San Jose : CEGESTI.

CEPAL ONU. (2002). *Globalización y desarrollo*. https://www.cepal.org/es/publicaciones/2724-globalizacion-desarrollo

Clavijo, C. (2014). Criminal compliance en el derecho penal peruano. *Revista de la Facultad de Derecho PUCP*, 625-647.

Crovi, D. (2005). La sociedad de la información. *Comunicaciones libres*, 23-37.

Cruz, R. (2020). Delitos imprudentes en el marco de las actividades empresariales. Una observación desde la cultura de la prevención. *Díkaion*, 226-245.

De la Cuesta, J. (2011). Responsabilidad penal de las personas jurídicas en el Derecho Español. *Revista Electrónica de la AIDP*(A-05).

EFE. (2018). *Apple deja de ser la empresa de mayor valor de mercado en el mundo*. Portafolio: https://www.portafolio.co/internacional/microsoft-es-la-empresa-mas-valiosa-del-mundo-523953

Elinor, M., & Molina, A. (2004). Análisis documental y de información: dos componentes de un. *ACIMED*.

Escobar, S. (2009). *La expanción del derecho penal -Análisis de las capacidades auto-restrictivas de los sistemas modernos del delito a partir de la libertad de expresión.* https://repository.urosario.edu.co/bitstream/handle/10336/1263/72345789-2009.pdf?sequence=1

Espinoza, M. (2017). Derecho penal informático: deslegitimación del Poder punitivo en la sociedad de control. *Tesis de grado*. Universidad Nacional del Antiplano: Puno.

Etxeberria, E. (2018). Las empresas como posibles responsables penales y los planes “compliance” como herramientas de solución. *Revista de Dirección y Administración de Empresas*, 52-74.

Fernández, C. (2018). La amenaza de las nuevas tecnologías en los negocios: El ciberespionaje empresarial. *Revista de Derecho UNED*, 17-56.

Frankz Alberto Carrera Calderón, J. E. (2019). Desafío de la ciberseguridad ante la legislación penal. *Revista Dilemas Contemporáneos: Educación, Política y Valores*.

Fung, B. (2021). *Amazon enfrenta una multa récord en la Unión Europea por violación a la privacidad*. CNN Español: https://cnnespanol.cnn.com/2021/07/30/amazon-multa-

privacidad-trax/?fbclid=IwAR2FNbcu5Bzsel2l2bamfhCMqVQ6WbquVpDuOE7KeA9_JkiA-A2XEf2dPMw

Garcia, P. (2012). Esbozo de un modelo de atribución de responsabilidad penal de las personas jurídicas. *REJ – Revista de Estudios de la Justicia – Nº 16 – Año 2012*, 55-74.

Henriksson, K. (2019). *¿Qué es un canal de denuncias?* WhistleB : https://whistleb.com/es/blog-news/what-is-a-whistleblowing-hotline/

Hernández, R., Fernández, C., & Baptista, M. d. (2014). *Metodología de la investigación .* Mc Graw Hill Education : https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Lefebvre · El Derecho S.A. (2022). *Microsoft desarticula la red cibercriminal ZLoader especializada en el robo y extorsión*. https://elderecho.com/microsoft-desarticula-la-red-cibercriminal-zloader-especializada-en-el-robo-y-extorsion

Mantilla, E. (2018). La empresa como instrumento en la comisión de delitos de cuello blanco. *Tesis de maestria*. Univerisdad Espiritu Santo: Samborondóm.

Mañas, V. (2016). Responsabilidad penal corporativa y cibercriminalidad. *Tesis de grado*. Valencia: Universidad de Valencia.

Martínez, M. (2006). *La investigación Cualitativa (Síntesis conceptual).* REVISTA IIPSI: https://sisbib.unmsm.edu.pe/bvrevistas/investigacion_psicologia/v09_n1/pdf/a09v9n1.pdf

Martínez-Martínez, D.-F. (2018). Unificación de la protección de datos personales en la unión europea: desafíos e implicaciones. *El profesional de la información*, 185-193.

Martínez-Padilla, M. (2015). La responsabilidad bancaria frente a los delitos informáticos. *Tesis de maestria*. Universidad Andina Simón Bolivar: Ecuador.

Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista Chilena de Derecho*, 235-260.

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Revista Ius et Praxis*, 159-206.

Mayer, L., & Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. *REVISTA CHILENA*, 151-184.

Montes, S. (2022). *Microsoft desarticula ZLoader, una red cibercriminal de alcance mundial*. Escudodigital: https://www.escudodigital.com/ciberseguridad/microsoft-desarticula-zloader-red-cibercriminal-alcance-mundial_51475_102.html

Navas, I., & Jaar, A. (2019). La responsabilidad penal de las personas jurídicas en la jurisprudencia chilena. *Política Criminal, 14*(28), 323-364.

Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Revista Nuevo Foro Penal*, 72-112.

Puerto, D. (2010). La globalización y el crecimiento empresarial a través de estrategias de internacionalización. *Pensamiento & Gestión, num 28*, 171-195.

Ramos, J. (2012). *La hipótesis en la investigación jurídica*. Instituto de Investigaciones Jurídicas Rambell: http://institutorambell.blogspot.com/2012/11/la-hipotesis-en-la-investigacion.html

Rayón, M. (2018). Los programas de cumplimiento penal: origen, regulación, contenido y eficacia en el proceso. *Anuario Jurídico y Económico Escurialense*, 197-222.

Reyna, L. (2016). Criminalidad informática, crimen organizado e internazionalización del delito. *Derecho Penal Contemporaneo – Revista Internacional*, 5-34.

Rincón, J. (2015). El delito en la cibersociedad y la justicia penal internacional. *Tesis Doctoral*. Universidad Complutense de Madrid: Madrid.

Ruedas, M., & otros, y. (agosto de 2009). *Hermenéutica: La roca que rompe el espejo.* SCIELO: http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1316-00872009000200009

Sánchez, I. R. (2016). La Sociedad de la Información,Sociedad del Conocimiento y Sociedad del Aprendizaje. *bibliotecas anales de investigación*, 235-243.

Santillana, R. (2021). *PROYECTO DE LEY. LEY DE SEGURIDAD INFORMÁTICA Y REPRESIÓN DE LOS DELITOS INFORMÁTICOS.* Congreso de la República : https://www.leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/Proyectos_Firmas_digitales/PL05630.pdf

Silva, J. (2006). *La expansión del derecho penal.* Buenos Aires : BdeF.

Villavicencio, F. (2014). Delitos Informáticos. *IUS ET VERITAS*, 284-304.

Zanata, A. (2016). *La responsabilidad penal de las personas jurídicas .* Universidad Internacional de La Rioja .