UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE DERECHO

ESCUELA ACADÉMICO PROFESIONAL DE DERECHO

TESIS

LA CRIMINALIDAD INFORMÁTICA O TECNOLÓGICA Y SUS DEFICIENCIAS LEGISLATIVAS EN EL DELITO DE ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS.

PARA OPTAR TÍTULO PROFESIONAL DE ABOGADO

Autor (es)

Bach. Carrillo Díaz, Cynthia Fiorella

Bach. Montenegro Dávila, Alicia Noemí

Asesor:

Dra. Uchofen Urbina, Ángela Katherine

Línea de investigación:

Derecho Penal

Pimentel - Perú

2018

Dedicatoria

A Dios por cuidar de mí, guiar mis pasos por el camino del bien.

A mi madre Teresa por ser padre y madre para mí, siendo un gran apoyo durante mi formación profesional, por su amor, confianza y ejemplo de superación, a mi tía Elvira por ser una segunda madre para mí, por quererme y apoyarme siempre, a mis hermanos Juan, Leslie y Julissa por la confianza brindada

Carrillo Díaz Cynthia Fiorella

A Dios por habernos permitido llegar hasta este punto y habernos dado la salud para lograr nuestros objetivos, además de su infinita bondad y amor; a mi madre Luz por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada por su amor; a mi padre Olegario por los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante; a mis hermanos Alex, Elizabeth y Matías, por estar conmigo y apoyándome siempre.

Montenegro Dávila Alicia Noemí

Agradecimiento

Este presente trabajo de tesis realizada en la prestigiosa Universidad Señor de Sipán, es un esfuerzo en el cual, participaron distintas personas, opinando, corrigiendo, acompañándonos en los momentos de crisis y en los momentos de felicidad. Lo cual nos ha permitido aprovechar la competencia y la experiencia de muchas personas que deseamos agradecer en este apartado.

A nuestra Coordinadora de la Facultad de Derecho, por brindarnos su apoyo incondicional junto con sus coordinadores de tesis.

Agradecer también a nuestros familiares que estuvieron dispuestos a darnos si ayuda y apoyo en este recorrido de nuestra carrera profesional.

Y en general a todas las personas y profesionales que directa e indirectamente nos impulsaron en la culminación de este trabajo de investigación, agradeciéndoles sus experiencias y conocimientos.

Las Autoras

INDICE

LA CRIMINALIDAD INFORMATICA O TECNOLOGICA Y SUS DEFICIENCIAS LEGISLATIVAS EN EL DELITO DE ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMATICOS.

Carrillo Díaz Cynthia Fiorella

Montenegro Dávila Alicia Noemí

Resumen

Ante la creciente ola de delincuencia que aqueja a la comunidad, han surgido diferentes modalidades delictivas, las cuales no están reguladas de una manera adecuada por el ordenamiento jurídico peruano, consecuentemente el Estado en el año 2013 promulga la Ley 30096 – Ley de Delitos Informáticos y en marzo del 2014 su modificatoria N° 30171, sin embargo esta no regula de manera precisa el delito de atentado a la integridad de sistemas informáticos, por ello dentro del objeto planteado se pretende analizar la criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos. Por otro lado planteamos la hipótesis haciendo referencia que si existen deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos los cuales no permiten determinar el bien jurídico protegido.

Finalmente se obtuvo como resultado que el delito informático de AISI, no determina el bien jurídico protegido, ya que es un delito que no se agota en la afectación al patrimonio, sino que muchas veces, por efectos de los daños ocasionados al sistema informático, el perjuicio se extiende más allá adquiriendo la naturaleza de un delito pluriofensivo que perjudica a la persona, el Estado y a la Sociedad.

Palabras Claves: la criminalidad informática, delito de atentado a la integridad de sistemas informáticos

Abstrac

In view of the growing crime wave that afflicts the community, different types of crime have arisen, which are not regulated in an adequate way by the Peruvian legal system, consequently the State in 2013 promulgates Law 30096 - Law on Computer Crimes and in January 2017 its amendment Law No. 30171, however this does not precisely regulate the crime of attack on the integrity of computer systems, so that within the general objective raised a legislative proposal was developed to protect the legal rights not protected in the crime of illicit access to a computer system typified in Law 30096. Therefore, within the general objective set out to analyze computer or technological crime and its legislative deficiencies in the crime of attack on the integrity of computer systems. On the other hand, we propose the hypothesis referring that if there are legislative deficiencies in the crime of attack to the integrity of computer systems then in that sense, we consider that all the behaviors or verbs must have as object of the action the functionality or operability of the computer system, proposing, consequently, the modification of article N ° 4 of Law 30096 and its amendment Law N ° 30171. Finally it was obtained as a result that the cybercrime of AISI, in itself, is not a crime that is exhausted in the affectation to the patrimony, but that, often, by effect of the damages caused to the computer system, the damage extends beyond acquiring the nature of a multi-offensive crime that harms the person, the State and society.

Keywords: *The computer crime, crime of attack to the integrity of computer systems.*

INTRODUCCIÓN

Los robos tecnológicos son capaces de penetrar cualquier sector de la red poniendo en riesgo cualquier dispositivo como se evidenció con las intromisiones en los sistemas de conducción de vehículos conectados con GPS o internet. Incluso las más avanzadas tecnologías de los vehículos autónomos se encuentran en riesgo de ser hackeados y controlados a distancia. En el 2015, los hackers ocasionaron choques entre autos al ingresar a su software con una computadora de uso común con la cual alteran la percepción de la realidad circundante al sistema de detección láser que está diseñado para frenar o maniobrar ante cualquier obstáculo. Por ello dentro del objetivo general planteado se pretende analizar la criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos.

La tecnología ha resultado sumamente útil para facilitar la comisión de muchos delitos tipificados. En algunos casos, no es necesaria una adecuación típica, pero en otros casos es necesario adecuar el tipo penal para abarcar la conducta que utiliza la tecnología. Ante ello la consecuencia más relevante del uso de la informática o la tecnología para afectar intereses jurídicos ajenos es la aparición de un bien jurídico nuevo necesitado y merecedor de protección. En consecuencia, la respuesta penal debe ser adecuada para cada una de las consecuencias constatadas.

La investigación servirá para la comunidad jurídica por ser un tema novedoso y acorde a la realidad nacional en relación a delitos informáticos, con una propuesta legislativa, buscando salvaguardar los intereses de las personas, de sus datos y sistemas informáticos.

En el Capítulo primero se desarrolló la situación problemática del estudio, donde abarca los aspectos como la situación problemática a nivel Internacional, Nacional y Local, la justificación e importancia, los objetivos y sus limitaciones. Por consiguiente en el Capítulo segundo se detalla el Marco Teórico, aquí se

encuentran los antecedentes de la investigación, el desarrollo de la temática correspondiente y la definición conceptual de la terminología empleada.

En el Capítulo tercero se describe el Marco Metodológico aquí se desarrolló el tipo de investigación, el diseño de la investigación, población y muestra, la hipótesis, variables, cuadro de operacionalización, métodos de investigación, técnicas de investigación, descripción de los instrumentos utilizados, análisis estadístico e interpretación de los resultados. Siguiendo en el Capítulo cuarto encontramos el análisis e interpretación de datos: detalla el análisis e interpretación de los resultados. En el Capítulo quinto se detallara la propuesta de investigación. Y en el capítulo sexto se denota las conclusiones y recomendaciones, además de la bibliografía y los anexos pertinentes.

CAPÍTULO I:

PROBLEMA DE INVESTIGACIÓN

I. PROBLEMA DE INVESTIGACIÓN.

1.1. Realidad Problemática

A nivel internacional

Augusto Bequai (1996), en su intervención Computer Related Crimes en el Consejo de Europa señala que: “Si continua el desorden político en todo el mundo, las redes globales de cómputo y los sistemas informáticos y de telecomunicaciones atraerán seguramente la ira de terroristas y facinerosos. Las guerras del mañana serán ganadas o perdidas en nuestros centros sistemas de cómputo, más que en los campos de batalla. En Orwell en el año 1984, los ciudadanos en Oceanía vivían bajo la mirada vigilante del Hermano Grande y su policía secreta. En el mundo moderno, todos nos encontramos bajo el ojo inquisidor de nuestros gigantes sistemas computacionales e informáticos”. En occidente, la diferencia entre el Hermano Grande y nuestra realidad es la política llamada democracia; al no existir ésta, el edificio electrónico para una implantación dictatorial ya existiría.

La revolución de la electrónica y de los sistemas informáticos ha dado a un pequeño grupo de tecnócratas un monopolio sobre el flujo de información en todo el mundo. En la sociedad informatizada, el poder y la riqueza están convirtiéndose cada vez más en sinónimos de control sobre los bancos de datos informáticos. Somos ahora testigos del surgimiento de una elite informática”. (Duran, 2002, p. 96).

De esta manera, la Organización para la Cooperación y el desarrollo Económico, en 1986 publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica, en donde se establecían las normas legislativas vigentes y las propuestas de reforma en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso

indebido que, los países podrían prohibir y sancionar en leyes penales (Lista Mínima), como por ejemplo el fraude y la falsificación informáticos, sabotaje informático, la alteración de datos y programas de computadora, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

La mayoría de los miembros de la Comisión Política de Información, Computadoras y Comunicaciones recomendaron también que se instituyesen protecciones penales contra otros usos indebidos (Lista optativa o facultativa), espionaje informático, utilización no autorizada de un programa de computadora protegido, utilización no autorizada de una computadora, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras. Con objeto de que se finalizara la preparación del informe de la Organización para la Cooperación y el desarrollo económico, el Consejo de Europa inició un amplio estudio sobre el tema a fin de elaborar propuestas que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección en los estados miembros.

A nivel nacional

El Estado en el año 2013 promulga la ley 30096 – Ley de delitos informáticos, considerando las penas y sanciones para los diferentes delitos expuestos en dicha norma.

Ante ello el fenómeno de la criminalidad informática en el Perú, delimita al bien jurídico lesionado por la delincuencia informática y examina su evolución legislativa en nuestro ordenamiento, cabe precisar que los delitos informáticos no pueden ser una actividad que se someta al

capricho temporal que vive día a día la sociedad y que está en constante crecimiento; por ende, se debe de aspirar a la creación de una ley más eficaz y amplia. El Perú no puede permanecer en el caso de que se tengan que sufrir consecuencias para dar resultados, la jurisprudencia debe de ayudar a una mejor legislación en cuanto a vacíos legales. (García, 2000, p. 145)

En los últimos tiempos la tecnología ha resultado sumamente útil para facilitar la comisión de muchos delitos tipificados. En algunos casos, no es necesaria una adecuación típica, pero en otros casos es necesario adecuar el tipo penal para abarcar la conducta que utiliza la tecnología.

La consecuencia más relevante del uso de la informática o la tecnología para afectar intereses jurídicos ajenos es la aparición de un nuevo bien jurídico necesitado y merecedor de protección. En consecuencia, la respuesta penal debe ser adecuada para cada una de las consecuencias constatadas.

1.2. Formulación del Problema

¿En la criminalidad informática o tecnológica existen deficiencias legislativas en relación al delito de atentado a la integridad de sistemas informáticos?

1.3. Objetivos de Investigación

Objetivos Generales:

Analizar la criminalidad informática o y tecnológica y las deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos.

Objetivos Específicos:

.

a) Analizar el marco teórico de la Criminalidad informática y el delito de atentado a la integridad de sistemas informáticos.

b) Determinar la legislación comparada en el delito de atentado a la integridad de sistemas informáticos.

c) Identificar los vacíos y las omisiones que posee la Ley de Delitos Informáticos en función al delito de atentado a la integridad de sistemas informáticos

d) Elaborar una Propuesta Legislativa, que modifique el delito de atentado a la integridad de sistemas informáticos, e incorpore circunstancias agravantes.

1.4. Justificación e importancia de la investigación

La presente investigación desde el modo práctico, se justifica debido a que dicha investigación será un aporte a las ciencias del Derecho, la cual está orientada con un tema que genera inquietud al Estado y a la Sociedad teniendo en cuenta que la criminalidad informática en el Estado peruano no está aún muy bien regulada, teniendo en cuenta que con la Ley 30096 no es precisa en función a la vulneración de sistemas informáticos y bases de datos, no regulando los siguientes bienes jurídicos, tales como: la seguridad e intangibilidad del tráfico de información en la red y la seguridad de las comunicaciones e información informáticamente tratada, siendo que este delito solo

protege la funcionalidad del sistema informático más no la información que se encuentra dentro de este.

Ante ello en el Perú, la LDI, en su art. 4, regula el delito denominado “atentado a la integridad de sistemas informáticos” (en adelante AISI). Sin embargo, tal como pretendemos demostrar en la presente investigación, producto de una pésima técnica legislativa, el legislador peruano, al no tener claro el objeto de la acción sobre el cual recaen los cuatro verbos rectores utilizados en el tipo penal, confunde por ratos, el AISI con los delitos de daños y, en otros momentos, con el delito de coacción. Perdiendo de vista, por lo tanto, el bien jurídico protegido y la naturaleza propia de este delito que forma parte del cibercrimen y, en consecuencia, de una nueva manifestación de la criminalidad.

La situación se agrava cuando, pese a encontrar su inspiración en el Convenio sobre Cibercriminalidad de Budapest 2001, el legislador no regula, tal como este lo establece, el modus operandi o el medio comisivo a utilizarse por el agente, perjudicando con ello el propósito de lograr establecer y definir de manera idónea el contenido o contorno preciso de la conducta penalmente relevante en este tipo penal.

Por otro lado la presente investigación buscara a través de la casuística internacional argumentar mejor dentro de su marco teórico, con el fin de orientarnos a un mejor análisis de los delitos en estudio, por lo que la motivación del cambio, en lo fundamental, trata de enfrentar y dar solución a un tema concreto, como es el de facilitar el aprovechamiento, en pro de la rápida reacción contra los delitos, de los modernos medios técnicos de detección y/o registro de la comisión de aquellos.

El beneficio de la investigación es que servirá a la comunidad jurídica por ser un tema novedoso y acorde a la realidad nacional en relación a delitos informáticos, con una propuesta legislativa que regule de manera directa las penas, buscando proteger los intereses jurídicos de las

personas, de sus datos y sistemas informáticos en el delito de atentado a la integridad de sistemas informáticos.

1.5. Limitaciones de la Investigación

1. El Estudio se limitará a analizar la criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos.

2. Estudio se efectuó en el periodo 2017

CAPÍTULO II:

MARCO TEÓRICO

II. MARCO TEORICO

2.1. Antecedentes de la Investigación

A nivel Internacional.

1. Ureta (2009) en su investigación en la ciudad de Guayaquil - Ecuador titulada: “Retos a Superar en la Administración de Justicia ante los Delitos Informáticos en el Ecuador.”, para optar el Título de Magister en Sistema de Información General, de la Escuela Superior Politécnica Del Litoral de Ecuador; expone su conclusión primera lo siguiente:

   “Ecuador ha dado sus primeros pasos en el desarrollo de iniciativas que permiten la investigación y sanción de los delitos informáticos, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte los entes y profesiones dedicados a su investigación”. (p. 94)

2. Guerra (2011) en su investigación en la ciudad de México titulada: “Delitos Informáticos-Caso De Estudio.”, para optar el Grado de Maestro, del Instituto Politécnico Nacional de México; expone su conclusión tercera lo siguiente:

   “Los delitos informáticos en México, no son exclusivos de la competencia en materia penal, la diversidad de delitos variará con respecto a las ideas que tengan las personas que hagan uso de medios tecnológicos para delinquir. La justicia no puede

reducirse sólo a aquellos quienes tienen los medios económicos para proteger su computadora con un mecanismo de seguridad o que en todo caso hayan tenido un descuido; esto podría ser que en todo caso, el que una computadora esté conectada a Internet significa que cualquiera puede justificadamente borrar o destruir archivos, sólo porque no está protegida por algún mecanismo de seguridad, o en su caso, no encuadraría con el delito como lo estipula la ley mexicana, dejando desprotegido a cierto sector de la sociedad". (p. 119).

3. Rodríguez (2011) en su investigación en la ciudad de Colombia titulada: "Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación.", para optar el Título de Doctorado, de la Universidad Nacional de Colombia; expone su conclusión tercera lo siguiente:

"En Colombia no existe una ley que determine específicamente tipos penales que definan los delitos que se presentan con mayor frecuencia en Colombia en las redes sociales, lo que es necesario para sancionar correctamente estas modalidades delictivas que afectan una sociedad completa". (p. 21)

4. Gonzales (2013) en su investigación en la ciudad de Madrid titulada: "Delincuencia Informática: Daños Informáticos del Artículo 264 del Código Penal y propuesta de reforma.", para optar el Título de Doctorado, de la Universidad complutense de Madrid; expone su conclusión tercera lo siguiente:

“La realidad ha evolucionado de tal manera que cuando se ataca un sistema informático no sólo se está produciendo un daño concreto para una persona, sino que se está vulnerando un nuevo bien jurídico, cuyo objeto no se ha sabido definir detalladamente todavía, pero que gira en torno a la seguridad de los sistemas informáticos y las redes de comunicaciones. Una sociedad interconectada, como la actual, debe tener un ordenamiento que sea consciente de la importancia de la herramienta que interconecta a la propia sociedad y la proteja, de tal manera que ataques que afecten a la integridad de esa red, no sólo se configuren como daños concretos a usuarios concretos, sino como un perjuicio para toda la sociedad en abstracto”. (p. 353)

5. Rincón (2015) en su investigación en la ciudad de Madrid titulada: “El delito en la cibersociedad y la justicia penal internacional.”, para optar el Título de Doctorado, de la Universidad complutense de Madrid; expone su conclusión primera lo siguiente:

“los ciberdelitos o delitos universales no sean conocidos por la Corte Penal Internacional de forma subsidiaria o residual, sino que, por el contrario, por tratarse de delitos Universales, es esta instancia de Derecho Penal Internacional quien cuenta con los requisitos y calidades para adelantar su persecución, siendo este órgano quien realice su investigación, juzgamiento y sanción, desde que se tenga conocimiento de su comisión, como instancia primaria, nunca subsidiaria, donde el objetivo claro es la aplicación del Ius Puniendi, ya no Estatal, sino Universal”. (p. 491)

A Nivel Nacional.

1. Romero (2005) en su investigación en la ciudad de Lima titulada: "Marco Conceptual de los Delitos Informáticos.", para optar el Título de Magister en Computación e Informática, de la Universidad Nacional Mayor de San Marcos; expone su conclusión primera lo siguiente:

   "Se puede afirmar que los delitos informáticos en el Perú, son todas aquellas conductas y acciones utilizadas por una persona o grupo de personas que con el pleno uso de su(s) facultad(es) físicas y mentales y, mediante el uso indebido de cualquier medio informático o telemático, tienden a provocar un perjuicio a cualquier persona natural o jurídica". (p. 85)

2. Vega (2010) en su investigación en la ciudad de Arequipa titulada: "Los Delitos Informáticos en el Código Penal.", para optar el Grado de Magister en Derecho Penal, de la Universidad Católica Santa María de Arequipa; expone su conclusión primera y octava lo siguiente:

   "El avance científico y tecnológico han acarreado aspectos positivos e importantes en nuestra sociedad en los últimos tiempos, motivo por el cual la interpretación tradicional de los delitos en nuestro código penal han quedado desfasados ante la aparición de estos delitos de nueva data como es la criminalidad informática". (En la actualidad son escasos los procesos penales relacionados con los delitos informáticos, los mismos que se encuentran tipificados en nuestro Código Penal vigente en los

artículos 207º “A”, 207º “B” y 207º “C” los cuales fueron incorporados en nuestro Código Penal vigente mediante Ley Nº 27309 “Ley que incorpora los Delitos Informáticos en el Código Penal” de fecha 17 de julio del 2000, motivo por el cual cabría la derogatoria de los artículos antes mencionados y que se efectúe un estudio minucioso de los tipos penales que pueden ser realizados por medios informáticos del Código Penal vigente, los cuales deben ser agravados debido al impacto que ocasiona en nuestra sociedad). (p. 138)

3. Sequeiros (2016) en su investigación en la ciudad de Huánuco titulada: “Vacíos Legales que Imposibilitan la Sanción de los Delitos Informáticos en el Nuevo Código Penal Peruano-2015.”, para optar el Título de Abogada, de la Universidad de Huánuco; expone su conclusión tercera lo siguiente:

   “Nuevas modalidades de negocios por internet, como el comercio electrónico es un claro ejemplo de cómo los delitos pueden aparecer de diversas formas, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de los diversos tipos de transacciones”. (p. 44)

4. Parra (2016) en su investigación en la ciudad de Lima titulada: “Proyecto Legal Para un Esquema Nacional de Ciber Seguridad.”, para optar el Título de Abogado, de la Universidad de San Martín de Porres de Lima; expone su conclusión primera lo siguiente:

La falta de proyección en esta materia podría ocasionar que los Estados sean víctima de cada vez mayores y peores incidentes, los cuales pueden ser evitados a través de un trabajo previo y coordinado, adecuando la tecnología a la nueva realidad en la que el ciber espacio forma parte de la vida cotidiana tanto del Estado como de los ciudadanos. Hemos encontrado evidencia de ataques cibernéticos al Perú, con lo cual se materializa la situación de vulnerabilidad en la que nos encontramos, si bien hasta donde sabemos, los daños no han sido de gran magnitud, eso no asegura que en un futuro los ataques que el Perú reciba puedan llegar a causar mayor daños. (p. 150)

5. Romero (2017) en su investigación en la ciudad de Huánuco titulada: “Delitos Informáticos Cometidos a Través de Redes Sociales y su Tratamiento en el Ministerio Publico en la Ciudad de Huánuco, 2016.”, para optar el Título de Abogado, de la Universidad Huánuco; expone su conclusión primera y segunda lo siguiente:

   Se debe realizar un análisis de la legislación penal vigente por parte del Organismo Legislativo en lo relativo a los delitos informáticos, a efecto de determinar si los tipos delictivos vigentes, alcanzan a cubrir todas las acciones que en la práctica atentan contra los sistemas informáticos y el uso adecuado de los mismos. El Ministerio Publico debe establecer un protocolo con procedimientos mínimos, para la recuperación de la evidencia informática y su evaluación pericial, el cual debe contener el perfil del perito informático, los procedimientos de recuperación de la evidencia informática, de su peritación y

requisitos del informe pericial, que permitan la confiabilidad de esta evidencia como medio de prueba. (p. 64).

A Nivel Local.

1. Samillan (2015) en su investigación en el departamento de Lambayeque titulada: “Incidencias sobre el delito de Grooming en Adolecentes: caso región Lambayeque.”, para optar el Título de abogado, de la Universidad Señor de Sipán; expone su conclusión generales lo siguiente:

   Los adolescentes del departamento de Lambayeque, se vieron afectados en sus derechos por los Empirismos Aplicativos e Incumplimientos a la Ley sobre delitos informáticos contra la identidad y libertad sexual que se encuentra regulado en la ley N° 30096 en el artículo 5, porque desconocen los Planteamientos Teóricos, especialmente los conceptos básicos, o por no cumplirse la Norma de nuestro ordenamiento jurídico o por no haber aprovechado las Legislaciones Extranjeras especialmente las de América que están más relacionadas con nuestra realidad, por parte de las instituciones públicas. (p. 129)

2. Morales (2016) en su investigación en la ciudad de Chiclayo titulada: “La Inseguridad al Utilizar los servicios de Redes Sociales y la Problemática Judicial para Regular los Delitos Informáticos en el Perú - 2015.”, para optar el Título de abogado, de la Universidad Señor de Sipán; expone su conclusión Octava lo siguiente:

Por ser una problemática de nivel mundial, esta delincuencia ha sido regulada internacionalmente tal es el caso del Convenio de Budapest, al cual no estamos inscritos, La Convención Internacional sobre la Delincuencia Cibernética, uno de los grandes problemas de toda clase de delincuencia es el de detectar el modus vivendi y operando del delincuente para así poderlo detener, por lo que una de las ciencias auxiliares del Derecho Penal para llevar a cabo esa finalidad encontramos a la Criminalística que enfocada a los Delitos Informáticos. (p. 121)

2.2. Bases Teóricas

2.2.1. La Criminalidad Informática o Tecnológica

2.2.1.1. Evolución histórica de la criminalidad informática o tecnológica.

La revolución tecnológica que comenzó en la segunda mitad del siglo xx es solo comparable, por sus impactos socioeconómicos, a la revolución industrial del siglo XIX. En efecto, la tecnología desarrollada después de la Segunda Guerra Mundial permite hablar de una “revolución tecnológica” en la cual la informática y, especialmente el microchip, es el elemento central que facilitó la creación de todos los aparatos de uso común en la vida diaria. Los cambios tecnológicos surgieron en el siglo XX, produciendo una trasformación de tal magnitud como los propiciados por la revolución industrial del siglo XIX. Impulsando la revolución tecnológica el desarrollo de los sistemas informáticos, en la cual la computadora dejó la oficina para invadir los hogares y abarcar todas las actividades y ocupaciones humanas. A ello se sumó el internet que permite el acceso remoto a cualquier sistema

informático, demostrándonos que la idea de Bill Gates (1999) que afirma que:

> *Ve el futuro conectado por una verdadera autopista de la información es ya una realidad de la cual gozamos, nos beneficiamos e incluso padecemos. Sin embargo, la tecnología no solo ha impactado favorablemente en la vida sino que también ha facilitado la aparición de nuevas formas de criminalidad. (pág. 59)*

2.2.1.2. El delito informático

Unos de los primeros temas a definir es el contenido del injusto del denominado “delito informático”, pues se trata de un término muy usado para definir conductas en las cuales se constata el uso de la informática o nuevas tecnologías que afectan diversos bienes jurídicos. Como se ha visto, muchos delitos pueden ejecutarse utilizando estas tecnologías sin afectar el principio de legalidad, pero también se constata que la informática determina la existencia de nuevas conductas, las cuales incluso afectan nuevos bienes jurídicos.

De acuerdo con Ulrich SIEBER (1998), el principal estudioso a nivel mundial de este tema, la denominación “computercrime” apareció inicialmente en los periódicos y en la literatura científica en los años 60. Recién un par de décadas más tarde, en la reunión de la OECD en l983 se aceptó la definición de “computercrime” o “computerrelatedcrime” (criminalidad informática o criminalidad relacionada con computadoras).

MORHRESCHLAGER (1994), por su parte, reconoce la dificultad de identificar adecuadamente las conductas de la criminalidad

informática, por lo que afirma que “no existe una definición legal” del delito informático. Luego, citando a WASIK (1991), “generalmente, el uso de la computadora en la comisión de un delito no altera el hecho de que el ilícito haya tenido lugar, es decir, no cambia la categoría del delito cometido”. (pág.53)

En la doctrina nacional, GARCIA CANTIZANO (2000) entiende que:

> *La “delincuencia informática comprende una serie de comportamientos que es difícil reducir o agrupar en una sola definición”, debido a que no hay un delito informático sino que solo es una forma de comisión. (pág. 79)*

REYNA ALFARO (2002) denomina “delitos computacionales” a todos los delitos que pueden ejecutarse con el uso de medios informáticos, mientras que los “delitos informáticos” son aquellos que afecta un nuevo bien jurídico. BRAMONT ARIAS TORREZ y MAZUELOS COELLO (2000), coinciden en que no existe una definición aceptada unánimemente sobre lo que es el delito informático, pero de modo general puede definirse como aquel que, para su comisión, se emplea un sistema automático de procesamiento de datos.

El profesor NUÑEZ PONCE (1996) los considera como “una nueva versión de delitos tradicionales”. Esta afirmación es parcialmente cierta pues, como veremos, un aspecto de la tecnología es servir como un nuevo medio de comisión, pero, por otro lado, se constata la aparición de nuevos bienes jurídicos y nuevas conductas propias de la era informática. La expresión “delito informático” se ha usado de manera coloquial extendiéndola a cualquier conducta en las cuales aparece la informática como

medio de comisión o cuando facilita la comisión del delito como la estafa difundida por internet o la pornografía infantil. (pág. 34).

Por otra parte, consideramos que se puede denominar delito informático cuando una conducta afecte un bien jurídico preciso y concreto que no se encuentre tradicionalmente protegido por el derecho penal, como la seguridad e intangibilidad de los datos almacenados, transmitidos o tratados informáticamente. En este caso, se puede hablar del "delito informático" como un delito autónomo. De esta manera, la definición de "delito informático", como expresión de la criminalidad informática, debe construirse en relación al nuevo bien jurídico que merezca protección y que excluye a las conductas que simplemente utilizan la tecnología o informática como medio para afectar bienes jurídicos diversos ya tutelados en el código.

En consecuencia, el uso de computadoras o nuevas tecnologías puede constituir un medio para afectar bienes jurídicos ya tutelados o denominarse "delito informático" cuando se afecte el nuevo bien denominado seguridad e intangibilidad de los datos almacenados, transmitidos o tratados informáticamente.

2.2.1.3. El nuevo bien jurídico lesionado por la criminalidad informática

A fin de verificar si el uso de la informática vulnera algún interés jurídico que merezca ser elevado a la categoría de bien jurídico penal, debemos, en primer término, identificar si las conductas que utilizan nuevas tecnologías o sistemas informáticos afectan bienes jurídicos ya tutelados o lesionan intereses nuevos que no son objeto de tutela; y, en segundo término, revisar si este nuevo interés cumple los requisitos de necesidad o merecimiento de

protección penal para ser reconocido por el derecho y elevado a la categoría de bien jurídico penal. (SILVIA SANCHEZ, 1992, P. 289)

Se constata que el uso de la informática y las nuevas tecnologías vulneran un nuevo interés que merece y necesita protección, el cual en el Perú, hasta el año 2000, no tuvo un tipo penal y, por ello, protección. En la ley colombiana, Ley N.° 1273, del 2009 se identifica a “la protección de la información y de los datos” es como el nuevo bien jurídico tutelado. De acuerdo a MAZUELOS COELLO (1997), se trataría de un bien jurídico “supraindividual vinculado a la seguridad e intangibilidad del tráfico de información en la red y propendería a garantizar la libre participación de las personas (usuarios) en la red”. REYNA ALFARO (2000) ha propuesto que el nuevo bien jurídico penal a tutelar sería “la información como valor económico de empresa”, el mismo que, a su juicio, cumple las exigencias de merecimiento de protección y necesidad de tutela.

Sin embargo, hay que tener en cuenta que la información con contenido patrimonial, datos sobre la intimidad, secretos industriales, secretos de Estado, o activos contables, valor económico de la empresa resulta insuficiente si no se encuentra almacenada, tratada, sistematizada o circula en la red. Si la información (o data en términos informáticos) representa o contiene valor económico nos referimos en realidad al patrimonio o la seguridad de las comunicaciones informática o telemática.

Por otra parte, consideramos que el bien jurídico informático que mencionados cumple los requisitos de necesidad de protección, importancia y trascendencia para la vida moderna, la seguridad o protección de datos informatizados o automatizados y que la ley de los delitos informáticos no los regula.

Siendo este el de: “seguridad y la intangibilidad de las comunicaciones e información informáticamente tratada o la seguridad de la información (o datos) que circulan en la red”

Consecuentemente se puede apreciar que dicho bien que no se encuentra tutelado busca cumplir con los requisitos de necesidad de protección y merecimiento de pena y que, además, no se encuentra adecuadamente protegido en la legislación nacional o extranjera; razón por la que este es el bien jurídico a proteger. Adicionalmente, también sería objeto de protección la confidencialidad de los datos.

Por otro lado la información, a secas, o la información que se encuentra fuera de un sistema informatizado no es el objeto específico de protección en las conductas que utilizan los sistemas informáticos. La información (almacenada o tratada fuera de los sistemas informatizados) tiene protección en los delitos contra la intimidad, violación del secreto profesional, la violación del secreto de las comunicaciones.

La seguridad de las comunicaciones e información informáticamente tratada o la seguridad de la información (o datos) que circulan en la red es el único que cumple los requisitos de necesidad de protección y merecimiento de pena.

Los delitos informáticos se encuentran sancionados en la Ley N.° 30096, Ley de Delitos Informáticos (LDI), dispositivo legal sancionador de índole penal que fue publicado en el diario El Peruano, el 22 de octubre del 2013. La investigadora considera que esta ley tiene una deficiente determinación del bien jurídico, situación que afecta la calificación penal y la imputación por parte del Ministerio Público; la ley busca proteger el aspecto físico del bien como es el sistema informático; además, cabe recordar que

conforme a la novena disposición final de la Ley N.° 30096, el sistema informático está constituido por los ordenadores y sus interconexiones. De esta manera el tipo penal está dirigido a la protección de un objeto físico y no un bien jurídico, pues entre ambos bienes existe una diferencia cualitativa: mientras una es el objeto físico en sí, lo otro es una cualidad genérica de todos los bienes físicos útiles para el desarrollo de la sociedad.

Esta diferenciación tiene consecuencias sustantivas en la regulación penal pues, al proteger un bien físico como el sistema informático, se desprotege los demás bienes tales como el sistema de transporte, el sistema de telecomunicaciones, etc., esto en virtud del principio constitucional que lo que no está prohibido está permitido, necesitando tantas normas como infinidad de bienes necesitan de protección legal. En cambio, cuando el tipo penal protege no al bien físico en sí, sino al bien jurídico, el aspecto jurídico de protección se hace extensivo a todo los bienes existentes, de esta manera bienes jurídicos como la propiedad, la integridad del bien, el desarrollo tecnológico, la indemnidad sexual, el honor, etc., se hacen extensivos a todos los bienes físicos corpóreos o incorpóreos, siendo suficiente un tipo penal para un bien jurídico y no la situación ilógica de regular un tipo penal para cada bien físico que siendo estos indeterminados tendríamos un número de normas también indeterminadas.

2.2.1.4. La cibercriminolgía y su relación con la seguridad e intangibilidad del tráfico de información en la red.

En la actualidad vivimos ante la cambiante dinámica económica, jurídico, social y cultural, debe servir como un análisis al Estado

para intervenir en la prevención y sanción de los delitos, analizando sus causas y consecuencias; puesto que cada día se incrementan las conductas delictivas, que son dañinas y, que afectan al Estado y a la sociedad, que son a menudo motivadas por diversos factores que se encuentran implícitas en el ambiente donde nace y se desarrolla los seres humanos como ser bio-psico-social.

Sin embargo, debido a los diversos avances y cambios tecnológicos que ha surgido en las diferentes formas de interactuar y propiamente de un fenómeno social que antes se situaba únicamente en la interacción social física, hoy vemos como esta ha sido reemplazada por la hiperconectividad de los sistemas informaticos y tecnológicos, con trascendencia global. (PEÑA LABRIN, 2014, p. 9)

En consecuencia, el surgimiento de las tecnologías de la información y comunicación (TIC) han abierto un campo de posibilidades para que surjan conductas con relevancia penal, que son criminológicas, aprovechado dicha situación con el fin de modernizar sus actividades criminales y valiéndose de las herramientas que la web brinda en el siglo XXI. (CAMPOS DELGADO & RAMIREZ VILCHEZ, 2013, p. 18)

Terceiro Morón Lerma (2014), quien nos precisa sobre el pasaje del homo sapiens a homo digitalis, destacando que: “en el ciberespacio, cada persona es potencialmente un emisor y un receptor en un medio cualitativamente diferenciado, en el que todos se comunican con todos pero, los internautas, no se localizan principalmente por su nombre, posición social o ubicación geográfica, sino a partir de centros de intereses, por lo que puede hablarse de una suerte de “mundo virtual segregado por la comunicación, lo que obliga a la criminología intentar

ponerse al día para formular nuevos perfiles criminales que respondan a las características suigéneris, de esta nueva criminalidad que avasalla el planeta". (PEÑA LABRIN, 2015, p. 150)

En ese sentido, Ulrich Beck precisaba que, "en un principio, la utilización de dicho concepto estuvo relacionada, principalmente, al ámbito de las ciencias básica, en términos de análisis y de la evaluación del desarrollo de las nuevas tecnologías". No obstante, por el hecho de que este tipo de evaluación avanzó mucho en términos de refinanciamiento y precisión, de manera inevitable, surgieron los conflictos sociales derivados de los peligros asociados al desarrollo de nuevas tecnologías. (PAULUS SANTIBAÑEZ, 2004, p. 1)

En Latinoamérica, para los cibercriminales representa una enorme oportunidad para obtener altas ganancias, debido a que en esta región existen economías más altas, que se encuentran entre las más importantes del mundo y, al mismo tiempo, el bajo riesgo que representa ser identificados, procesados y sentenciados por la escasa criminalización informática versus la efectiva criminalización que existe en EE. UU. Y en la Unión Europea.

Siendo que por un lado el aspecto positivo de las tecnologías de la información y comunicación admiten herramientas útiles de interconexión proporcionando un mejor desarrollo para el mundo, resaltando la inteligencia artificial que antes era propia del cerebro humano; (sin embargo, desde un punto de vista negativo, traen consigo una serie de potenciales peligros para el sector empresarial y para adultos y, principalmente para los niños, niñas y adolescentes quienes son posibles víctimas de la demencia digital o sistemas informáticos, a menudo por falta de

capacidad y suficiencia para discernir las verdaderas intenciones de las personas con quienes sostienen relaciones virtuales, vulneración de sistemas de seguridad, de tal forma que analizando este tema podremos entender y conocer las verdaderas dimensiones y el desarrollo de los medios informáticos (cibernética), el uso del internet y las computadoras, con las que día a día nos relacionamos tal vez sin percibir sus consecuencias). (VASQUEZ ROCCA & ZIGMUNT BAUMAN, 2008, p. 5)

En tal sentido, como bien refiere Pérez Luño, las TIC “han posibilitado que los seres humanos de nuestro tiempo puedan establecer una comunicación sin límites en el espacio, sin límites en las personas y en tiempo real. Internet constituye la gran revolución de nuestro tiempo y sus efectos se proyectan también en la esfera de las libertades [...], han propiciado nuevas formas de ejercicios de los derechos y pueden contribuir al reforzamiento del tejido participativo de las sociedades democráticas”. (PEREZ LUÑO, 2012, p. 23)

En el Perú se cuenta con la División de Investigación de Delitos de Alta Tecnología de la DIRINCRI – PNP, pero sin embargo su trabajo, pese a sus esfuerzos, es insuficiente por la falta de apoyo logístico, presupuesto y posicionamiento en la sociedad, unido a ello la cifra negra que aún pesa en esta gama de delitos, que muy a pesar que existe una Ley de delitos informáticos, esta no establece cuando estamos frente a un delito informático o cuando estamos ante un delito tipificado en el Código Penal.

Por otro lado debemos precisar que el progreso de la informática es una de las características primordiales y destacadas de los últimos milenios, por lo que la utilización de este, comprende unas diversas posibilidades que son indispensables delimitar a

fin de combatir los excesos que se vienen apreciando. (BLOSSIERS HUME, 2004, p. 271)

El desarrollo de las de las tecnologías de la información y comunicación han permitido comunicarse a distancia por vía electrónica, revolucionado la forma de comunicarnos entre nosotros, permitiendo que sean cada vez más las personas que tienen acceso a las mismas acortando la brecha digital de los sistemas que aun constituye un óbice al desarrollo. Si bien la utilización de estas trajo ventajas significativas, también vino aparejada del surgimiento de sucesos delictivos, por el inadecuado uso de las mismas, ya que no existen límites de lo permitido o no en la red. De aquí surge el cuestionamiento: "¿existen el tiempo y el espacio en el ciberespacio? Evidentemente no, cualquier persona desde cualquier lugar del mundo puede cometer un delito o conducta desviada contra otra online, basta con que tenga una conexión a internet. Asimismo, ¿las víctimas son más vulnerables? También la respuesta es que sí, porque el ciberespacio es un lugar desconocido, un lugar en el que se puede engañar mejor, porque existe el anonimato, la posibilidad de ser cualquier persona y sobre todo, la eventualidad de hacer creer cualquier cosa a cualquiera en cualquier lugar del mundo". (GONZALES GARCIA, 2013, p. 40)

Pedofilia, pornografía infantil, verbigracia, phishing, grooming, sexting, usurpación de identidad y amenazas por medio de correos electrónicos y redes sociales, entre otros, son ejemplos planteados con un cristalino examen de la realidad pluricausalista y multifactorial en la que estamos viviendo y a lo que nos enfrentamos cotidianamente. En palabras de Susana Tomasi:

"Phishing: Técnica utilizada para captar datos bancarios de los usuarios a través de la utilización de la imagen de la entidad

bancaria. [...] Cuando se faciliten datos bancarios a través de internet es fundamental comprobar que se trata de páginas web con protocolos de seguridad válidos [...]. El phishing es una técnica de captación ilícita de datos personales (principalmente relacionados con claves para el acceso a servicios bancarios y financieros) a través de correos electrónicos o páginas web que imitan/copian la imagen o apariencia de una entidad bancaria/financiera (o cualquier otro tipo de empresa de reconocido prestigio) [...]".

"Sexting: Consiste en el envío de contenidos de tipo sexual (principalmente fotografías y/o videos) producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles".

"Sexting: Consiste en el envío de contenidos de tipo sexual (principalmente fotografías y/o videos) producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles".

El gran desarrollo y expansión de los sistemas de la información y comunicación ha comenzado a surgir nuevas temáticas y desafíos respecto a la seguridad informática, ya que organismos de gobierno, las empresas, e individuos adaptados a la era digital, se han encontrado con personas inescrupulosas se aprovechan de una manera inadecuada de dicha tecnología para cometer delitos, conductas desviadas, usufructuarla en su provecho y, fraudes o apropiarse de información almacenada , por lo cual se hacen necesarios nuevos tipos de investigaciones.

"Se llama grooming, a la acción deliberada de un adulto de acosar sexualmente a un niño o niña mediante el uso de internet. Siempre es un adulto quien ejerce el grooming. Estos adultos

suelen generar un perfil falso en una red social, sala de chat, foro u otro, en donde se hacen pasar por un chico o una chica y entablan una relación de amistad y confianza con el niño o niña que quieren acosar. El mecanismo del grooming suele incluir un pedido de foto o video de índole sexual o erótica (pedido por el adulto, utilizando el perfil falso). Internet es una herramienta que brinda nuevas posibilidades a problemáticas previamente existentes".

Como bien destacan García Flores y Reyes Pérez (2008), "reflexionar en torno al horizonte de sentido entre la modernidad y la posmodernidad es reconocer una compleja transición, se trata así mismo de un tiempo histórico de ausencia de luz que nos permitiera al menos de alguna manera advertir hacia donde se orienta dicha transición o tendencia histórica". (p. 57)

Siendo que la posmodernidad viene a ser un concepto muy amplio que se refiere a una tendencia de la cultura, el arte y la filosofía que surgieron a finales del siglo pasado. "A nivel general, puede decirse que lo posmoderno se asocia al culto de la individualidad, la ausencia del interés por el bienestar común y el rechazo al racionalismo". "El movimiento posmoderno, a grandes rasgos sostiene que la modernidad falló al pretender renovar las formas de pensamiento y expresión. Por eso se asocia al desencanto y la apatía ya que parte de lo entiende como un fracaso de la sociedad".

Respecto a la posmodernidad, explica Bernardo Del Rosal lo siguiente:

"Es sujeto a gran controversia, en el extremo que hay quien ha sugerido que su uso excesivo lo ha vuelto en exceso frágil. Lo postmoderno hace referencia a algo nuevo y diferente que ha

sucedido en los últimos tiempos y que ya no puede ser explicado en términos de 'modernidad'. Por lo que, más que definir el contexto vigente, quizás la clave está en precisar si las recientes o, las inminentes reformas penales son continuidades del pasado o, por el contrario, asistimos a verdaderas discontinuidades que rompen con ese pasado y que están dando origen a algo nuevo, a algo distinto, frente a lo que, por tanto, tenemos que adoptar un enfoque analítico y una estrategia diferente ante la modernización de la criminalidad. [...] (El discurso de la modernidad en el derecho penal, a lo largo de todas sus fases de desarrollo (interna y externa), ha significado, básicamente, el discurso de la convicción en que el comportamiento criminal es una conducta anormal e indeseable, pero evitable, y el discurso de confianza en que a través del adecuado soporte o de las adecuadas técnicas de intervención, el ser humano es capaz de modificar, reorientar o inhibir sus comportamientos criminales). (DEL ROSAL BLASCO, 2009, p. 57)

2.2.1.5. Extensión de la criminalidad informática

Para comprender la extensión de la criminalidad es necesario analizar lo señalado por Mateo Girón:

[...] Bauman lo describe como la nueva irrelevancia del espacio como el paso a la modernidad liviana, disfrazada como aniquilación del tiempo. En primer lugar, "el desarrollo de los medios de comunicación que permiten, para quien los maneja, la "casi instantaneidad" en una escala global, así como la invisibilidad de esos usuarios para con quien no tiene acceso a dichos medios". En segundo lugar, "implica la pérdida de valor del territorio [en sentido estricto]. El espacio tiene un valor

fetiche, en términos del George Simmel, el espacio vale lo que cuesta y hoy en día puede neutralizarse miles de kilómetros en horas" [...] (ZYGMUNT BAUMAN, 2013, p. 11)

En esa línea, Fernando Miró Llinares (2011) indica lo siguiente sobre los delitos informáticos o cibercrímenes:

Hace referencia que el vocablo cybercrimen, provienen de la unión del prefijo cyber, derivado del término cyberspace, y el término crimen, como concepto que sirve para englobar la delincuencia con relación al uso de las Tecnologías de la información y comunicación [...]. En los estudios jurídicos sobre la criminología han sido llevados a cabo en inglés, imponiendo este término frente a otros que ocupan generalmente el mismo significado, tales como computercrime y otros en lo que se utilizan prefijo como virtual, online, high-tech, digital, computer-related, Internet-related, electronic y e-crimes. ((p. 7)

Por su parte, el internet, está siendo utilizado como medio de comunicación por los ciudadanos del mundo, ha dado lugar a múltiples tendencias, una de ellas es la proliferación, como dijimos, de conductas desviadas y delictivas donde los cibernautas se comunican en línea a todo nivel; sin embargo, diversos comportamientos están orientadas a ocasionar daño a cuantiosas empresas, personas, jóvenes y menores de edad que a menudo interactúan sin conocimiento o ingenuidad.

Es un problema que surge de la utilización de la información electrónica y medios de comunicación en la tierra, a consecuencia del incremento de la tecnología informática y de comunicación como internet, correos electrónicos, Facebook, Instagram, Twitter, Whatsapp, blogs, websites, y democratización universal de los smartphone, etc., los cuales pueden ser el móvil

para acercarse y dañar a un individuo o grupo social, mostrando un comportamiento deliberado, repetitivo y hostil, valiéndose de las TIC para la comisión de cualquier delito cibernético.

Bajo ese contexto, en la criminología existe una especialidad que es la cibercriminología que se ocupa necesariamente de conocer cómo influyen las actividades online en la vida offline de las personas, por lo que la Universidad Miguel Hernández de Elche (España, 2013), realizó encuentros internacionales con los máximos expertos en esta materia, llegados de Australia, EE. UU., Argentina, Inglaterra y España, la temática se centró en averiguar cómo influye el ciberespacio en la configuración de la delincuencia en la sociedad, si es un facilitador de determinadas tipologías delictivas y qué características aporta en la delincuencia. Asimismo, para el año 2017 se realizará la Conferencia Internacional en Cibercrimen y Computo Forense (ICCCF por sus siglas en inglés), abordando las nuevas modalidades delictivas del siglo XXI.

Por lo que podemos observar actualmente, que los ataques más comunes siguen centrándose en intereses económicos contra sectores financieros de uso diario por la clase media. Por ello, los intentos iniciales en crear acciones preventivas son enfocados a clientes y cuentahabientes de las instituciones bancarias, notándose una inversión económica significativa en años recientes por parte del sector privado, siendo que mientras que la parte de las autoridades han invertido fuertes cantidades de tiempo y diseño en campañas de advertencia en el uso de la información que se proporciona por medios no físicos para su identificación, con el fin de hacer uso de sus cuentas financieras personales.

Estos esfuerzos con buenas intenciones probablemente han hecho más cautelosos a miles de potenciales víctimas; sin embargo, mientras las campañas mantenían un mismo formato a través de los años, el uso de internet se intensificaba de manera progresiva, llegando a la era de la conexión permanente a través de dispositivos móviles, generando un nuevo problema que ha tomado su tiempo identificar: el ingreso del cibercriminal a equipos de uso diario donde la información personal y profesional se encuentra almacenada en un mismo lugar, comprometiendo no solo la seguridad financiera de quien pierda el control (material o digital), sino también su integridad física. “Es lo que ocurre con el ciberespacio como ámbito social que tiene como caracteres intrínsecos una concreta configuración de las coordenadas espacio/tiempo, frente a la que tiene en el que podríamos denominar espacio real o físico. (MIRO LINARES, 2015, p. 5)

La localidad del derecho debe ceder frente a la globalidad de la red, incluso en ámbitos como el derecho penal y procesal que siempre estuvieron tan ligados a la soberanía de carácter territorial.

Al respecto, Miró Llinares (2015) afirma lo siguiente:

Se suele utilizar, como sinónimo de ciberespacio, al concepto de “espacio virtual”, como antitético al espacio “real”. La simultaneidad, la unicidad de momentos, puede llevar a la impresión de que el ciberespacio es la ausencia de espacio, quizás fruto del equívoco de asimilar la idea de espacio a la distancia. No obstante, el ciberespacio es real en el sentido que existe, pero se trata de una “especie nueva” de espacio, invisible a nuestros directos sentidos y en el que las coordenadas de

espacio y tiempo adquieran otro significado y ven redefinidos su alcance y límites. (p. 6)

La volatilidad del web 2.0, traducidas en la evolución de las redes inalámbricas y del propio hardware móvil, las cámaras digitales y los videos grabadoras, es cada más accesible para los cibernautas de las grandes mayorías, así como de los sistemas de defensas bancarios y financieros, lo cual ha creado una nueva faceta de cibercrimen que debe identificarse rápidamente para hacerle frente a la mutación del delito.(PEÑA LABRIN, 2012, P. 144)

Es en este punto donde la participación de la cibercriminología se vuelve crucial, ya que mientras los equipos tecnológicos mantienen un avance constante, el investigador solo se ha especializado en la operación de estos, sin prestar atención de forma prioritaria al comportamiento criminal en el ciberespacio y considerando que pueden identificarse de forma previa algunas conductas que ayudarían a su prevención antes de que el hecho sea amenazado o vulnerado, afectando los bienes jurídicos tutelados por la ley penal y las leyes especiales.

2.2.1.6. Legislación comparada

Estados Unidos

El Acta Federal de Abuso Computacional de 1994, que modificó el Acta Fraude y Abuso Computacional de 1986, diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques

de virus, de aquellos que lo realizan con la intención de estragos. (Ramírez, 2016, p 23)

Como el autor expresa, el acta de Estados Unidos fue modificada llegando a plantear diversas medidas de sanción para regularizar los virus que contaminen bases de datos, ya que al destruir, trasmitir o cambiar los sistemas informáticos, estos se consideran como delitos, es por tal motivo que la ley impuesta se semejó al problema dando cabida a una nueva era de ataques tecnológicos.

El Acta define dos niveles para el tratamiento de quienes crean virus, estableciendo para aquellos que intencionalmente causan daño por la trasmisión de ese virus, el castigo de hasta 10 años en prisión más una multa y para aquellos que lo trasmiten, solo de manera imprudencial la sanción consiste de entre una multa y un año en prisión.

Los legisladores estadounidenses, la nueva Ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delito, la nueva Ley da lugar a que se contemple que se debe entender como acto delictivo. (Bierce, 1994, p. 20)

Para el autor, Estados Unidos es como un país en donde existen con facilidad la irregularidad de los medios informáticos en donde la ley regulada guarda nexo con el problema planteado, en donde cambia la figura del delito por la palabra acto delictivo.

En el Estado de California, en 1992 se llega adoptar la Ley de Privacidad en donde se contemplan los delitos informáticos pero en menor grado que los delitos guardando relación con la intimidad la cual se constituyen como el objetivo principal de esta Ley. (Ramírez, 2016, p. 23)

Para el autor Ramirez el objeto de la Ley es la protección del individuo con respecto a la base de datos y a los sistemas computarizados ilegales, en donde la protección legal es base para la protección de la intimidad de los individuos, dando bienestar al Estado de California.

Colombia

Andrés Velásquez, presidente y fundador de la compañía de cibert Seguridad Informática, expresa que existen dos tipos de cibert, aquellos que llegan a realizar un delito aprovechando de que saben sobre las vulnerabilidades de los sistemas informáticos y aquellos que se encargan de robar información de la empresa o base de datos con el fin de utilizarla para beneficio propio, muy a pesar que no son expertos con la tecnología. (Huerta, 1990, p.19)

El problema más presentado por el autor frente a la comunidad colombiana es la suplantación de identidad, difamación por internet, fraude cibernético, denegación de servicios, fuga de información, entre otros. Ahora bien estos problemas son consecuencia los hackers tal como lo demuestran los medios de comunicación, pero para la compañía Cibert estos problemas llegan a vulnerar la privacidad individual y empresarial.

El Congreso de la Republica de Colombia bajo la Ley 1273 dado el 5 de Enero de 2009, llega a sancionar, protegiendo la información y datos de sistemas tecnológicos de información y comunicaciones. (García, 2009, p, 16)

Para el autor esta norma se llegó a convertir como protección de un bien titulado estableciendo una normatividad de conductas delictivas relacionadas a la tecnología a través de medios informáticos, en donde el país de Colombia pasó a ser el pionero a nivel mundial en materia de legislación de delitos informáticos.

Actualmente existe la Ley 1273 en donde estos delitos son castigados con pena de prisión que equivalen a las 48 y 12 meses y multas de hasta 1,000 salarios mínimos legales mensuales vigentes, pero para algunos expertos expresan que mientras existen más creaciones de normas que generen soluciones a problemas, están surgiendo más tecnología para burlarse de ellas.

Venezuela

Aquellas conductas que son sancionadas por el derecho haciendo un mal uso del medio informático, existe una ley en Venezuela que se encarga a pasos agigantados de la regulación de una área tecnológica en donde las actividades sin ser ilícitas presentan una plaga a la sociedad. (Pérez, 1996, p. 41)

Para el autor en Venezuela hay leyes que se encargan de regular el ambiente tecnológico sin embargo hay algunos que a pesar de que no sean ilícitos estos presentan consecuencias a la sociedad

entre ellas tenemos: Acceso Indebido, sabotaje o daño a sistemas, Espionaje informático, falsificación de documentos, manejo fraudulento de tarjetas inteligentes o instrumentos análogos, difusión o exhibición de material pornográfico, apropiación de propiedad intelectual, etc. Estas actividades antes mencionadas llegan o no estar tipificadas como delitos, sin embargo hace un gran daño a la sociedad.

Panamá

Teniendo como imagen España acerca de la penalidad por usurpar la identidad o lesionarla, la Policía Nacional se preocupó por reforzar el tema denunciado el uso incorrecto de las redes sociales, autores como el abogado Jorge Torregrosa (2004), indica que los delitos informáticos se encuentran tipificados en el Código Penal, imponiendo en el Código sanciones que llevan a la prisión aproximadamente seis años, esta conducta se encargará de la regulación de los delitos informáticos. (p, 29)

Como bien expresa el abogado la legislación de Panamá verso mucho en casos de España, en donde los delitos se encuentran tipificados de acuerdo al Código Penal, esta Ley tiene que determinar la responsabilidad de los imputados como también identificar los daños cibernéticos.

Las normas establecidas y adoptadas mediante la ley 26 del 2008, la Ley 5 de 2009, la Ley 68 de 2009 y la Ley 14 del 2010 Título VIII Delitos contra la Seguridad Jurídica de los medios electrónicos Capítulo I Delitos contra la seguridad Informática que

va desde el articulo 289 hasta el artículo 291. (Davara, 1993, p. 15)

Ecuador

Se inició a través de los primeros tipos penales informáticos en el año 2002 en donde surgió el proyecto para la creación de la Ley de comercio electrónico, los cuales posteriormente fueron incluidos en el Código Penal, esto se pensó luego de que pasará los primeros ataques en el año 2001 fuera de la página del Municipio de Quito, tomando como referencia el primer delito que se cometido en el año 1996, cometido por EMETEL. (Nuñez, 19998, p. 26)

Para el autor Ecuador dio inicio de la proyección de medios informáticos cuando en este surgió ataques en Quito, dándose la creación de la Ley de comercio electrónico, actualmente ejerciéndolo como un procedimiento técnico en donde participan expertos en la materia, teniendo como ayuda alguna asistencia penal internacional para recabar la información respectiva.

La Ley 67, publicada el 17 de abril del 2002, tiene un avance muy importante en el sentido de incluir figuras penales que castiguen los ilícitos informáticos, con lo cual junto al Código Penal integran normas creadas para la sociedad de la información. (Avellán, 2010, p.20)

Dentro de estas normas promulgadas en la Ley 67 para posteriormente ser trascritas al Código Penal, constan los siguientes ilícitos informáticos:

Art 57 LCEFEMD: Infracciones informáticas.- son aquellas que tienen carácter administrativas y se encuentran tipificadas en el Código Penal, en la presente Ley.

Art. 58 LCEFEMD, Conc. Art 202.1 CP: Contra la Información Protegida.- aquella persona que quiere acceder o vulnerar información y también la seguridad de dicha información será reprimida con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Esta Ley permite establecer lineamiento jurídicos a través de las normas, incluidas el comercio electrónico en donde se encarga de cuidar los principios de confidencialidad y la reserva de los mensajes de datos, sin llegar a violar los principios de intuición electrónica.

México

En el Código Penal Federal de México, dedica un capítulo del noveno título de su segundo libro" ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA", en donde de se establece la protección de las comunicaciones. (Téllez, 2004, p. 29)

Como expresa el autor se requiere de políticas que ayuden a implementar una sana relación entre el individuo con la tecnología, llegando a la investigación y persiguiendo delitos, reuniéndolos en una misma Ley Federal.

2.2.1.7. Casos más relevantes a nivel mundial

Caso Herbert Zinn

a) Fue el primer sentenciado bajo el cargo de Fraude Computacional y Abuso en 1986

b) Tenía 16 cuando violo el acceso a AT&T y los sistemas del Departamento de Defensa

c) Destrucción del equivalente a US $174,000 en archivos, copias de programas.

d) Sentenciado a 9 meses de cárcel y a una fianza de US$10,000.

Caso David Smith

a) Acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo

b) Pena de hasta diez años de cárcel.

c) Contamino a más de 100,000 ordenadores de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas estadounidenses como la del Gobierno

Caso Kevin Poulsen

a) Acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar.

b) Encara hasta 10 años en la cárcel.

c) Conocido por su habilidad para controlar el sistema telefónico de Pacific Bell.

d) Crackeó todo tipo de sitios, pero él se interesaba por los que contenían material de defensa nacional.

2.2.1.8. Tipos penales afectados por la criminalidad informática.

Las nuevas conductas pueden clasificarse en: i) delitos informáticos, cuando se afecta el nuevo bien jurídico merecedor y necesitado de protección; y ii) un nuevo medio que facilita la comisión de delitos previstos en el Código Penal o las leyes penales, haciendo la precisión que en algunos casos se tendrá que reformar el tipo penal para poder subsumir la nueva conducta a la ley penal.

La razón usual para reformar los tipos penales es el objeto material referido a un objeto corpóreo que no se condice con la nueva realidad informática.

a) Difamación

(Art. 132 del CP) El tipo penal agravado de difamación se justifica en el mayor desvalor de la acción por la capacidad de difundirse

el agravio a una extensa cantidad de personas a través de “si el delito se comete por medio del libro, la prensa u otro medio de comunicación social […]”. Esto es, se requiere que la versión injuriosa se difunda sobre un medio de comunicación social, el cual se referiría a los medios tradicionales como la prensa escrita, radial o televisiva. Sin embargo, en la actualidad las Tecnologías de la información y de la comunicación han introducido una variedad de medios informáticos, redes sociales, correos electrónicos, Twitter, blogs o páginas web que reúnen dos características centrales para propagar las noticias como i) capacidad de soportar archivos con información en cualquier formato sea audio, escritos o video y ii) capacidad de difusión incluso mayor que los medios clásicos de información, pues con su publicación en una web o en un blog, la noticia o comentario es capaz de ser visto por un número indeterminado de personas.

Por ello, para evitar lagunas de punibilidad que afecten el principio de legalidad, debido a que se puede interpretar la prensa como publicaciones periódicas, usualmente escritas, y que los medios de comunicación tradicionales no engloban las nuevas vías de difusión se debe reformar este artículo para incluir una fórmula que comprenda a los nuevos medios tecnológicos como se hace en el Código Penal español “cualquier medio de eficacia semejante”.

b) Violación de la intimidad (art. 154 del CP)

La violación de la intimidad se encuentra definida como el acceso o interferencia, indebida, de aspectos de la intimidad personal mediante instrumentos o procesos técnicos que permitan observar o registrar hechos o imágenes. En la agravante, el

concepto de “medio de comunicación social” puede ser interpretado como he señalado en la difamación agravada, por lo que para incluir a todas las formas de comunicación o difusión de información a través del internet o las redes sociales se pueden emplear la fórmula “cualquier medio de eficacia semejante”.

c) Violación de correspondencia, supresión o extravío indebido de correspondencia y publicación indebida de correspondencia (arts. 161, 163 y 164 del CP)

La principal limitación para adecuar a estos tipos penales para reprimir las manifestaciones de la delincuencia tecnológica es el objeto material. Se restringe a la “correspondencia epistolar o telegráfica”, de escaso uso, como el objeto sobre el cual recae la acción, esto es, que los actos de supresión o extravío solo pueden recaer en comunicaciones escritas como cartas o mensajes. Estos delitos se configuraron en la época pre internet cuando las comunicaciones se efectuaban básicamente mediante el papel, por lo que la expresión “u otro de naturaleza análoga” limita la interpretación únicamente a aquellos que tienen como soporte el papel; es decir, que el tipo penal protege únicamente a las cosas corporales o tangibles. Esto es, debido a que la interpretación correcta a la expresión que contiene el art. 161 “otro de naturaleza análoga” es asimilar a otros elementos similares o parecidos a la carta, pliego o telegrama o despacho telefónico que tengan como soporte el papel.

En consecuencia, corresponde modificar este tipo penal para incluir en el objeto material a las comunicaciones interpersonales

que se realicen por cualquier medio que utilice la informática y las tecnologías de información (TIC).

d) Delito de escucha indebida (art. 162 del CP)

La norma señala que el objeto material es una “conversación telefónica o similar”, lo cual se restringe a las comunicaciones de voz, pues se refiere a las comunicaciones similares entre las que únicamente pueden ser las transmisiones de voz. En consecuencia, se excluyen otras transmisiones que se realizan con las nuevas tecnologías de información.

e) Interferencia de comunicaciones electrónicas (art. 162-B del CP)

Este tipo introducido en 2015 pretende cubrir la desprotección que tenían las comunicaciones modernas, por ello, hubiera sido preferible establecer el objeto material relacionado a las tecnologías de la comunicación (TIC) para incluir a los medios modernos de comunicación que han sido introducidos por la informática o las tecnologías de la información.

f) Delito de turismo sexual comercial infantil y adolescente en el ámbito de turismo (art. 181-A del CP)

Esta modificación incluyó a internet como medio de difusión para difundir o promover la explotación sexual de menores, aunque sería conveniente realizar una modificación para utilizar una

fórmula más amplia e incluir cualquier forma de comunicación que utilice las tecnologías de la información.

g) Delito de publicidad de prostitución sexual infantil (art. 182-A del CP)

Se refiere a los responsables, esto es, director o editor de los medios de comunicación, pero se excluye a los de las páginas web o de otros medios de comunicación electrónica.

h) Exhibición o publicación obscena (art. 183 del CP) y pornografía infantil (art. 183-A del CP)

La exhibición a menores de material pornográfico puede realizarse “por cualquier medio”, con lo cual se incluye la internet, pero en el delito de pornografía infantil se incluye expresamente la internet. Sería conveniente utilizar el uso de la tecnología de la información o comunicación que traen otras y nuevas formas de transmisión de información. Con este artículo se incorpora la difusión de material pornográfico realizado por cualquier medio de distribución incluyendo la internet u otros medios de difusión.

La Ley de delitos informáticos del 2013 perfeccionó esta conducta al ampliar los medios de difusión a los elementos que ofrecen las tecnologías de la información, lo cual brinda un espectro más amplio que la informática o la internet. Las tecnologías de la información (TIC) o tecnologías de la información y comunicación se refieren a recursos que se desarrollaron a partir de la computadora e internet.

i) Delitos contra el patrimonio

Delito de hurto telemático (modalidad agravada contenida en el art. 186, segundo párrafo, inc. 3 del CP) Las afectaciones del patrimonio individual fueron las primeras manifestaciones de la criminalidad informática, pero no se podían sancionar por los delitos tradicionales que protegían este bien jurídico. Los delitos de hurto encontraban una limitación respecto a la cosa mueble como objeto de apropiación.

Las cosas o bienes muebles aptas para ser el objeto material en el sentido que expresa el art. 185 del CP, especialmente en el denominado “hurto telemático” en la transferencia electrónica de fondos, son, precisamente, los fondos entendidos como activos o dinero electrónico, pero cuando la norma penal se refiere ampliamente al uso de la telemática, se trata de cualquier elemento informático con valor económico y que forma parte del patrimonio individual. (ROJAS VARGAS, 2000, P. 284)

El delito de hurto telemático funcionó perfectamente hasta su derogación por la Ley de delitos informáticos del 2013. A partir de esta ley, la protección del patrimonio fue protegido por el nuevo tipo de estafa informático.

Delito de estafa En principio, se debe tener en cuenta que el tipo penal de estafa es una obra en tres actos se construye sobre los siguientes elementos: i) engaño u otra forma fraudulenta; ii) error; y iii) perjuicio patrimonial. Por ello, no era apto para afrontar el uso de la tecnología para apropiarse del patrimonio ajeno. La Ley N.° 30096, Ley de delitos informáticos del 2013, derogó el hurto telemático y erigió el tipo de estafa telemático, según el modelo español, sobre la base de la “manipulación informática” para obtener un beneficio económico. • Delito de daños Un sector de

la doctrina propone la reinterpretación del delito de daños para afrontar los problemas del sabotaje informático a partir de considerar que ese tipo penal no exige la materialidad de la cosa mueble o inmueble que se traduzca en “aprehensividad”, en el sentido de los delitos de apoderamiento. Lo verdaderamente relevante, nos informa GUTIERREZ FRANCES es que “se deteriore o dañe algo valorado económicamente” con lo cual se puede incluir a los elementos lógicos de los sistemas informáticos como objeto material del delito de daños. La Ley N.° 30096, Ley de delitos informáticos del 2013, introdujo los atentados a los soportes lógicos.

j) Delitos contra los derechos de autor y conexos (arts. 216, 217 y 219 del CP)

El uso de la informática y la tecnología constituyen medios útiles y eficaces para afectar el bien jurídico. Además, se han incluido expresamente en los arts. 220-A, 220-B y 220-C del CP a las conductas que utilizan medios tecnológicos para desactivar los mecanismos de seguridad que se colocan en las obras para, precisamente, evitar su copia o distribución ilegal.

k) Delito contra la fe pública

En conclusión, el documento electrónico reúne los requisitos establecidos por la doctrina: i) es un método de perpetuar y constatar el contenido; ii) medio de garantía para conocer al autor; y iii) sirve como prueba de su contenido. (Taboada, 2009)

En el Decreto Legislativo N.° 681 (14-10-91) se reconoce que los elementos o formas procesadas por sistemas tecnológicos o

informáticos tienen la calidad de documento con igual valor de los elaborados en papel. En la misma norma se determina que la falsificación y adulteración de micro formas o sus duplicados serán reprimidas como delito contra la fe pública.

2.2.2. El delito de Atentado a la integridad de sistemas informáticos

2.2.2.1. El tipo penal de atentado a la integridad de sistemas informáticos.

EL tipo penal de atentado a la integridad de sistemas informáticos. Para tales fines, se recurre a una interpretación sistemática de la norma penal, la lógica deductiva, la legislación comparada y la doctrina internacional que informa uno de los fenómenos mundiales de mayor trascendencia en la actualidad: el cibercrimen. De esta manera, devela los vacíos y las omisiones que esta norma posee en su contenido y, además, advierte las incoherencias que existen entre sus elementos, y las que subyacen entre la norma y la legislación penal ordinaria.

Desde que Robert Tappan Morris, estudiante de 23 años de la Universidad de Cornell de los Estados Unidos, infectara el 2 de noviembre de 1988 con el primer ejemplar de malware autorreplicable, un gusano informático, que afectó gravemente el funcionamiento de nada menos que 6, 000 ordenadores de un total de 60, 000 del sistema total de internet de dicho país, incluido la NASA, pasaron 12 años para que en el Perú se incorpore tímidamente, mediante la Ley N.° 27309, la figura de los delitos informáticos (arts. 207-A, 207-B, 207-C y 207-D del CP) y 25 años

para que se promulgue la Ley de Delitos Informáticos, Ley N.° 30096 (en adelante LDI). (Diario Gestión, 2016)

El delito de atentado a la integridad de sistemas informáticos, nomenjuris adoptado por nuestra legislación en la Ley de Delitos Informáticos, es conocido dentro de otras legislaciones como sabotaje o daño informático, el cual, forma parte de una gama de delitos que tienen en común el uso de las tecnologías de la información y comunicación para su comisión.

2.2.2.2. Precisión terminológica

Si revisamos la doctrina y la legislación internacional que trata del estudio y regulación de uno de los fenómenos mundiales que día a día toma dimensiones descomunales como la cibercriminalidad, podremos comprobar que el tema que pretendemos abordar, el delito de AISI, nomenjuris adoptado por nuestra legislación en una ley especial, la LDI, es conocida dentro de otras legislaciones como sabotaje o daño informático, el cual, forma parte de una gama de delitos que tienen en común el uso de las tecnologías de la información y comunicación (en adelante TIC) para su comisión.

2.2.2.3. Tipo Penal

En ese orden de ideas, lo que pretendemos en la presente investigación es el minucioso estudio crítico del art. 4 de la nueva LDI, el cual regula lo siguiente:

> *El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la*

prestación de sus servicios, será reprimido con una pena privativa de la libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

2.2.2.4. Antecedentes Legislativos

El Código Penal, hasta antes de la promulgación de la LDI, el 22 de octubre del 2013, regulaba dentro del Título V "De los delitos contra el patrimonio", en el Capítulo X, lo que denominaba "delitos informáticos". Así, el antecedente inmediato y directo del tipo penal en comento es el derogado art. 207-B del CP, el cual expresamente reprimía lo siguiente:

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

Como podemos advertir, de la lectura del derogado art. 207-B del CP, se regulaba dentro de un mismo tipo penal a dos delitos que a la fecha son independientes uno del otro en la LDI. El primero, el delito de atentado a la integridad de datos informáticos, contemplado en el art. 3 de la Ley de delitos Informáticos; el segundo, el delito de AISI contemplado en el art. 4 del mismo cuerpo normativo.

Ya hemos establecido el antecedente nacional del AISI. Entonces, ¿cuál es el antecedente internacional? Al respecto, podemos señalar que el legislador, en este tema, ha seguido las pautas establecidas en el convenio, el cual, luego de establecer en su

artículo primero las definiciones de “datos” y “sistemas informáticos” (recogidas íntegramente por nuestra legislación) procede en su art. 4 a señalar los lineamientos que cada Estado Parte debe regular en su legislación interna para reprimir el AISI, entendiendo por esta a “[…] la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos”.

2.2.2.5. Definición de sistemas informático en el derecho penal

“Sistema informático” es un concepto complejo y amplio que trasciende al derecho en general y más aún al derecho penal, por cuanto por él, en la informática, se entiende a todo el conjunto de partes, dispositivos, recursos, materiales e inmateriales que permiten almacenar, ordenar, procesar datos e información mediante la ejecución de programas, sistemas operativos orientados al apoyo de determinada actividad humana.

En ese sentido, no solamente comprende al hardware y el software, sino que además comprende al propio personal técnico encargado de crear y mantener el sistema en sí y, por último, a los propios usuarios finales.

Así, frente a este concepto tan omnicomprensivo y amplio, el legislador peruano, siguiendo la definición establecida en el apartado “a” del art. 1 del convenio, en la novena disposición complementaria de la LDI, procede a definir a sistema informático como:

"todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa".

En ese orden de ideas, dentro del derecho penal peruano, debe entenderse como sistema informático, a la parte física o corpórea del sistema, esto es, el hardware. El componente material, el cual está conformado por sofisticados dispositivos (técnicos-electrónicos) de entrada, salida, unidad central o de procesamiento y demás accesorios que conforman en su conjunto, una unidad operativa, la cual tiene como función el procesamiento, la interpretación, y ejecución automática de datos y de los componentes lógicos del sistema informático, todo ello, mediante la ejecución de un determinado programa, esto es, de un software.

2.2.2.6. Naturaleza Físico – Patrimonial del sistema informático

Así definido el sistema informático, dentro del campo penal peruano, dada su naturaleza física o corpórea, podemos deducir que nos encontramos frente una especie del amplio género bien mueble. Novísimo, moderno, sofisticado, pero al final un bien mueble, el cual por su utilidad, dentro de la automatización de la producción, posee indefectiblemente una valoración económica y patrimonial, constituyendo, dentro del sistema industrial, empresarial y comercial, una pieza fundamental del activo de una persona jurídica y del patrimonio de una persona natural. (GALGANO, 2005, pág. 20).

Anotando, como todos los sabemos que el género bien mueble, mucho antes de la promulgación de LDI, ya era objeto de

protección jurídica en el derecho penal peruano bajo el rubro de los delitos contra el patrimonio. Así, el delito de AISI constituye, por decirlo de algún modo, un delito de daño específico.

En el caso del Perú, atendiendo a la concreta tipificación establecida en el art. 4 de la LDI, podemos señalar que el bien jurídico protegido es la integridad, el acceso y la funcionabilidad o prestación de sus servicios del sistema informático. Resulta obvio que además de bienes específicamente propios del delito informático, se afecta el patrimonio del titular del sistema informático afectado.

2.2.2.7. Interpretación del tipo penal de AISI

2.2.2.7.1. Bien Jurídico

El delito informático de AISI, en sí, no es un delito que se agota en la afectación al patrimonio, sino que, muchas veces, por efecto de los daños ocasionados al sistema informático, el perjuicio se extiende más allá adquiriendo la naturaleza de un delito pluriofensivo. Así, coincidimos cuando De la Mata y Hernández (2009), sostienen que lo que se protege son intereses de contenido económico, los cuales no deben identificarse con el patrimonio en sentido estricto, por cuanto en un delito de esta naturaleza

> *"las consecuencias económicas principales y más graves no se limitan a la de la pérdida del valor económico de los datos afectados, sino que se expanden al perjuicio para, por ejemplo, la actividad empresarial que se esté llevando a cabo". (pág. 327)*

Además, debe agregarse que en algunos casos se afecta el normal abastecimiento o prestación de los servicios públicos, la seguridad nacional, etc. Más adelante, agregan los autores españoles, un enfoque desde la trasnochada concepción jurídica económica resulta a la fecha insuficiente, razón por la que debe trabajarse desde una perspectiva funcional que comprenda tanto la integridad como la disponibilidad de la información contenida en redes o soportes informáticos (concepto funcional de propiedad y patrimonio), entendiéndose que se afecta "la posibilidad de disponer en todo momento, de modo íntegro y con plena funcionalidad operativa, de los datos, programas y sistemas con los que operamos en nuestra vida, privada o pública, diaria" (DE LA MATA Y HERNADEZ, 2009, pág. 33).

En el caso del Perú, atendiendo a la concreta tipificación establecida en el art. 4 de la LDI, podemos señalar que el bien jurídico protegido es la integridad, el acceso y la funcionabilidad o prestación de sus servicios del sistema informático. Resulta obvio que además de bienes específicamente propios del delito informático, se afecta el patrimonio del titular del sistema informático afectado. Más adelante analizaremos las falencias de la tipificación.

Respecto del bien jurídico protegido en los delitos informáticos, ya hemos sostenido que la doctrina internacional no es pacífica. De la Mata y Hernández, efectuando un excelente resumen respecto de la postura de reconocidos autores, sostienen que, en los delitos informáticos, lo que se protege es: (la información y la accesibilidad a la información; la accesibilidad y la integridad de la información y de los sistemas informáticos; simplemente la información; la seguridad de los sistemas informáticos, entendida como el derecho a no sufrir injerencias externas en los datos,

programas o sistemas informáticos, por la trascendencia que estos tienen para el desarrollo mundial; la comunicación pacífica a través de las redes telemáticas, con independencia, se dirá, de las garantías y protección que pueden ofrecerse a otros bienes jurídicos como la intimidad o la protección a datos de carácter personal; la confianza en el funcionamiento de los sistemas informatizados, como interés de carácter supraindividual, de los que dependen todas las actividades tanto públicas como privadas; o incluso, directamente, la tecnología de Internet, bien jurídico, se dirá, de primera magnitud) (DE LA MATA BARRANCO Y HERNÁNDEZ DÍAZ, 2009, pág. 328).

2.2.2.7.2. Tipicidad objetiva

a) Sujeto activo:

El delito de AISI (conforme a la definición contenida en el tipo penal y en el anexo terminológico) es un delito común, en cuanto no requiere en el agente una calidad especial, un conocimiento o título especial, o que sea portador de un deber especial preexistente, o tenga la calidad de posición de garante de los sistemas informáticos involucrados (este supuesto es una agravante conforme el art. 11.2 de la LDI).

b) Sujeto Pasivo:

Toda vez que nos encontramos frente a una especie calificada de daños materiales a bienes muebles, el sujeto pasivo del delito será el propietario del sistema informático. El sujeto pasivo de la acción

será el posesionario o usufructuario legítimo del sistema informático objeto material del delito. Sin embargo, cabe preguntarse si los beneficiarios directos del buen funcionamiento del sistema informático (por ejemplo, diseñado para brindar algún servicio público o industrial) pueden también ser considerados como agraviados en determinados casos. Creemos que, considerando la trascendencia que acarrea el daño físico en perjuicio de terceros ajenos al propietario, posesionario o usufructuario, esta hipótesis no debe ser descartada.

2.2.2.7.3. Tipicidad Subjetiva

a) Modalidad Culposa

A diferencia de otras legislaciones, debemos señalar que, en el Perú, el tipo penal no admite en el AISI, en ninguno de los cuatro verbos rectores, una modalidad culposa. Ello, por cuanto exige en el agente una acción deliberada e ilegítima, resaltando con el primer término, de manera innecesaria, la exigencia de una conducta dolosa. Agregado a ello, debe tenerse en cuenta que, al no tipificar de manera expresa el AISI culposo, debe atenderse al segundo párrafo del art. 12 del CP.

b) Modalidad Dolosa

Se exige en el agente, en todos los casos, que actúe con plena conciencia y voluntad de inutilizar, impedir, entorpecer o imposibilitar el acceso, el funcionamiento o la prestación de sus servicios del sistema informático. Respecto de este punto, debemos advertir algo muy interesante, atendiendo que nos

encontramos frente a un tipo penal que regula un daño físico con resultados subsecuentes inutilización del sistema informático y que este daño final puede realizarse de la manera clásica (golpeando, mojando, estropeando física y directamente los dispositivos), o a través del uso de las TIC (mediante el uso de virus, gusanos, troyanos, etc.), resulta importante advertir que, en la primera modalidad, al evaluarse la conducta del agente, debe atenderse a la configuración del dolo trascendente, es decir, que el dolo no se agote en la conciencia y voluntad inmediata de dañar materialmente los componentes físicos del sistema informático, sino que debe acreditarse que el móvil o propósito final del agente estaba dirigido a inutilizar, impedir, entorpecer o imposibilitar el acceso, el funcionamiento o prestación de sus servicios del sistema informático.

2.2.2.7.4. Condición objetiva de punibilidad

Por otro lado, atendiendo que los verbos rectores recaen sobre un objeto material (entiéndase dispositivo informático), efectuando una interpretación restrictiva, debe exigirse, en el caso concreto, que no en todos los supuestos nos encontraremos frente al delito en comento, para ello debe requerirse que el dispositivo físico electrónico, informático, perteneciente a las TIC debe encontrarse en buenas condiciones, funcionando o brindando efectivamente determinado servicio. De no ser así, consideramos que nos encontraremos frente a un delito imposible, o tentativa inidónea, siendo que las conductas deben ser tratadas dentro de la figura penal que regula el delito contra el patrimonio daños. En efecto, tal como tendremos la oportunidad, más adelante, de revisar la tipicidad subjetiva, el tipo penal, requiere en el agente un dolo específico, el cual es pretender con su conducta inutilizar o

impedir el acceso al sistema informático, por un lado; y, de otro, entorpecer o imposibilitar el funcionamiento o la prestación de los servicios que venía prestado el dispositivo o sistema informático.

La inclusión del segundo verbo típico impedir no es la más feliz, por cuanto, al confundir hardware con software, no logra distinguir lo que es un delito informático (impedir el acceso al sistema lógico, al programa, a los datos del sistema), con lo que no pasaría de ser un delito contra la libertad coacción (impedir físicamente el acceso al sistema informático, entendido este como las partes físicas del sistema, el hardware).

2.2.2.8. Deficiencias Legislativas

Dentro de las deficiencias legislativas advertidas en el tipo penal en comento, siguiendo los aportes de la doctrina internacional y la legislación comparada, podemos advertir que el legislador nacional, absolutamente ajeno y de espaldas a los principios de mínima intervención del derecho penal, no ha regulado los parámetros que establezcan un control adecuado a efectos de poder identificar la conducta penalmente relevante.

2.2.2.8.1. Ausencias del criterio de valoración económica.

Por otro lado, el legislador no ha establecido un criterio de valoración económica o pecuniaria del daño objetivamente causado al sistema informático para cuantificar, valorar y determinar, ante un caso concreto, si nos encontramos frente a una infracción administrativa o ante una conducta penalmente relevante. Esta omisión resulta preocupante, por cuanto a la fecha

toda conducta que incurra en alguno de los cuatro verbos rectores y afecten el acceso o funcionamiento del sistema informático, aunque sea de manera leve, temporal o no, se encuentra penalizada: ello en grave perjuicio de la ya abundante carga procesal que soporta la administración de justicia.

2.2.2.8.2. Ausencia de criterio de gravedad de daños

Por otro lado, si consideramos que lo trascendente no es el daño patrimonial, sino la potencialidad para vulnerar intereses de carácter supraindividual, si renunciamos a una consideración estrictamente económico-patrimonialista del delito en comento, advertimos que el legislador tampoco ha utilizado otros criterios para determinar una escala valoración de la gravedad (leve, grave o muy grave) de los daños ocasionados, ya sea al propio sistema informático, o de valoración de la gravedad de los efectos o consecuencias acarreadas a partir del referido daño. Ello, con el propósito de distinguir, como en el caso anterior, si nos encontramos frente a una falta administrativa, propia del derecho administrativo sancionador, o frente a un delito pasible de una sanción penal.

La legislación española ha establecido como pautas para determinar la relevancia penal o no de la conducta incriminada una valoración de las consecuencias que se deriven, en perjuicio de terceros, y que tengan como origen los daños ocasionados al sistema informático por el agente. Así, se sanciona cuando como consecuencia de los daños ocasionados al sistema informático se afecten la normal provisión de servicios públicos esenciales de una colectividad (servicios de salud, seguridad, económicos); se

afecten la provisión de bienes de primera necesidad (alimentos, agua, energía eléctrica, gas natural); se afecten al sistema de seguridad del Estado o de una comunidad en general. Alemania, por su parte, regula la relevancia penal de una conducta cuando se afecta de manera esencial una empresa o industria ajena.

2.2.2.8.3. Omisión respecto de la titularidad de sistemas informáticos

Respecto de este punto consideramos que, si bien es cierto, lege lata, el sistema informático constituye un bien mueble y forma parte del patrimonio, ya sea de una persona natural o jurídica, en principio, lo que debería sancionarse es cuando el agente dañe un sistema informático que no es de su propiedad. Esta es la regla general que el legislador no ha previsto y debe ser subsanada. Sin embargo, toda vez que nos encontramos frente a un delito informático, el cual trasciende el bien jurídico propiedad, consideramos que, legeferenda, la eximente estipulada en el art. 20.10 del CP no debe resultar aplicable cuando, a pesar de que el sistema informático es de propiedad del agente, el daño trasciende los ámbitos de sus dominios y causen un grave perjuicio en agravio de terceros.

El legislador no ha establecido un criterio de valoración económica del daño objetivamente causado al sistema informático para cuantificar y determinar si nos encontramos frente a una infracción administrativa o una conducta penalmente relevante. Esta omisión resulta preocupante en tanto toda conducta que incurra en alguno de los cuatro verbos rectores y afecte el acceso o funcionamiento del sistema informático (así sea leve, temporal o no) se encuentra penalizada.

2.2.2.8.4. Delito de Daños Versus el delito de AISI

¿El delito de AISI puede ser considerado una especie del delito de daños? ¿Cuáles son los encuentros y desencuentros entre ambas figuras penales? Si consideramos que el art. 205 del CP, dentro de los delitos contra el patrimonio, al sancionar el delito de daños, reprime con una pena privativa de la libertad no mayor de tres años a "el que daña, destruye o inutiliza un bien, mueble o inmueble, total o parcialmente ajeno" y a esta norma penal la concordamos con el art. 4 de la LDI "el que […] inutiliza total o parcialmente el sistema informático", podemos comprobar, como primera observación, que ambos tipos penales utilizan el verbo "inutilizar".

Luego, cuando Salinas Siccha. (2013), trabaja el delito de daños, advierte que:

"inutilizar consiste en provocar la pérdida de la capacidad del bien para ejercer la función normal que le compete, sin que haya lesión en el aspecto material" (pág. 1281).

Concepto perfectamente aplicable al delito de AISI. Estas son las razones y las coincidencias por la que resulta pertinente establecer algunos lineamientos para saber cuándo estamos frente al delito de daños y cuándo frente al delito de AISI. Para ello, debemos formular algunas hipótesis provisionales de trabajo que luego vamos a desarrollar. Primero: Tanto el delito de daños (art. 205 CP) como el delito de AISI (art. 4 LDI) tienen como objeto de la acción penal a bienes muebles. Segundo: El delito de daños, a diferencia del delito de AISI, establece que el bien mueble objeto de la acción penal debe ser total o parcialmente ajeno. Tercero: El

delito de daños, a diferencia del delito de AISI, establece un criterio económico para diferenciar una falta de un delito. Cuarto: Lege lata, ante un caso de daños materiales a bienes muebles, el criterio para diferenciar, el delito de AISI del delito de daños, debe atenderse a la naturaleza informática o no del bien mueble objeto material del delito. Quinto: El delito de AISI adolece de serias deficiencias en su regulación, por cuanto no ha definido el medio comisivo que lo diferencie del delito de daños común. Sexto: La pésima técnica legislativa en el delito de AISI permite incluso (sino estamos atentos) confundirlo por momentos con el delito de coacción.

Dicho lo anterior, vamos a desarrollar una interpretación del AISI de lege lata. Luego vamos a trabajar sus falencias, vacíos y omisiones. Finalmente vamos a proponer una lege ferenda.

El delito de atentado a la integridad de sistemas informáticos es un delito compuesto por cuanto tiene hasta cuatro verbos rectores en el siguiente orden: inutilizar, impedir, entorpecer e imposibilitar, los mismos que no son convergentes (no se requiere la concurrencia de los cuatro verbos para la configuración del ilícito penal, basta la concurrencia de uno de ellos) ni excluyentes.

2.2.2.8.5. Confusión: delito de coacción versus el delito de AISI.

El delito de AISI, conforme el art. 4 de la LDI, establece como una de las cuatro conductas penales: el impedir el acceso al sistema informático. ¿El acceso de quién? Debe entenderse del operador informático. ¿El acceso a qué? ¿Debe entenderse al sistema lógico virtual, el acceso a los datos del sistema? (Resulta obvio, nos encontramos en un delito informático). Pero, la cuestión es

que, al haberse definido sistema informático como un bien mueble, no se podrá negar que también resulta válido interpretar que lo que se reprime, además, es el acceso del operador informático al sistema informático, entendido este último como el dispositivo electrónico, el bien mueble, el hardware del sistema informático. Es esta última interpretación la que nos preocupa, por cuanto guarda alguna relación con el delito de coacción al impedir hacer a alguien, lo que la ley no prohíbe (art. 151 CP).

2.2.2.9. Legislación comparada en función al delito de AISI.

En Italia, con una mejor técnica legislativa, se regula el delito de daños a sistemas informáticos o telemáticos, en el art. 635 donde se reprime penalmente a quien “mediante las conductas mencionadas en el artículo 635 del CP (la destrucción, deterioro, cancelación, alteración o supresión de datos, informaciones o programas) o a través de la introducción o la transmisión de datos, informaciones o programas informáticos destruya, dañe o inutilice en todo o en parte sistemas informáticos o telemáticos ajenos, u obstaculice de manera grave su funcionamiento”.

En España, el delito de daños informáticos en tipo básico se regula en su art. 264 del CP, el cual señala “el que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado […]”, estableciéndose agravantes en el mismo artículo. Luego, en el art. 264, reprime a quien, “sin estar autorizado y de manera

grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno".

En Francia, se reprime bajo el nombre de "atentados contra los sistemas de tratamiento automatizado de datos", y se regula al delito de daños en dos tiempos: en el art. 323-1 del CP, el acceso fraudulento y si producto de dicho acceso resultare la supresión o modificación de datos contenidos en el sistema o se produjera una alteración de su funcionamiento; luego en su artículo 323-2, se reprime el hecho de obstaculizar o alterar el funcionamiento de un sistema de tratamiento automatizado de datos.

CAPÍTULO III

MARCO METODOLÓGICO

III. MARCO METODOLÓGICO.

3.1. Tipo y diseño de la investigación

3.1.1. Tipo de investigación

La presente investigación es de tipo Descriptiva – Analítico.

Es descriptivo porque describe los datos y características de la población o fenómeno en estudio. También determina cual es la situación en la que se encuentra el objeto estudiado.

Analítico: Porque se analizó el marco teórico, relacionados con la criminalidad informática y el delito de atentado a la integridad de sistemas informáticos para encontrar las deficiencias legislativas.

3.1.2. Diseño de la Investigación

En cuanto al diseño de la presente investigación es No experimental y Transversal

Para Ñaupas et al (2014) se utiliza una muestra (M), la observación o medición de una variable (O), además de ello existe un tiempo en el que transcurre la investigación (T) y por último, el coeficiente de correlación (r).

Los “estudios que se realizan sin la manipulación deliberada de variables y en los que sólo se observan los fenómenos en su ambiente para después analizarlos”, El texto Metodología de la investigación, de Hernández, (2003).

Al no ser un experimento, aquí no vamos a manipular o controlar ninguna de las variables ni obtener variaciones mediante esta manipulación. (p. 331-341)

Es transversal o transaccional porque recogemos la información en un solo tiempo, en este caso, en un año aproximadamente.

Ñaupas et al (2014) “Se utiliza investigaciones transversales, en vez de hacer un seguimiento de una variable, durante 5 o más años, se estudia esa variable simultáneamente en un solo año.” (p. 343).

3.2. Población y Muestra

3.2.1. Población:

Se considera como población para efectos de la presente investigación, los Jueces, Los fiscales y los Abogados especialistas en Derecho Penal del Distrito Judicial de Lambayeque.

3.2.2. Muestra:

Por ser una población finita se toma, a la vez, como muestra a una parte de la población total. Considerándose como muestra no probabilística por conveniencia aplicada a 45 personas, divididas en 15 Jueces, 15 Fiscales, y 15 abogados del Distrito Judicial de Lambayeque.

3.3. Hipótesis

Si existen deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos entonces en ese sentido, consideramos que la norma no es clara en función al bien jurídico protegido, situación que afecta la calificación penal y la imputación por parte del Ministerio

Público, en consecuencia, es recomendable la modificación del artículo N° 4 de la Ley 30096.

3.4. Variables

3.4.1. Variable Independiente

Criminalidad Informática o Tecnológica:

De acuerdo con Ulrich Sierber, el principal estudioso a nivel mundial de este tema, la denominación “computer crime” apareció inicialmente en los periódicos y en la literatura científica en los años 60. Recién un par de décadas más tarde, en la reunión de la OECD14 en l983 se aceptó la definición de “computer crime” o “computer related crime” (criminalidad informática o criminalidad relacionada con computadoras).

Es una nueva versión de delitos tradicionales”. Esta afirmación es parcialmente cierta pues, como veremos, un aspecto de la tecnología es servir como un nuevo medio de comisión, pero, por otro lado, se constata la aparición de nuevos bienes jurídicos y nuevas conductas propias de la era informática. (Nuñez, 1996, p.40)

3.4.2. Variable Dependiente:

Delito de atentado a la integridad de sistemas informáticos:

el delito de AISI, nomenjuris adoptado por nuestra legislación en una ley especial, la LDI, es conocida dentro de otras legislaciones como sabotaje o daño informático, el cual, forma parte de una gama de delitos que tienen en común el uso de las tecnologías de la información y comunicación (en adelante TIC) para su comisión, el cual regula lo siguiente:

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

3.5. Operacionalización:

VARIABLES	DIMENSIONES	Técnicas e instrumentos
Variable Independiente: Criminalidad informática y tecnológica.	- Delito informático. - El bien jurídico lesionado por la criminología. - Legislación comparada. - Código Penal	La técnica es la bibliografía, para recoger información secundaria, relacionada con antecedentes, marco teórico y otros aspectos de las variables objeto de estudio
Variable Dependiente: Atentado a la integridad de sistemas informáticos.	- Tipo penal - Naturaleza - Legislación comparada - Ley 30096	La técnica es la encuesta, a través del cuestionario aplicado a los Jueces, Fiscales y abogados del Distrito Judicial de Lambayeque

3.6. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

3.6.1. Los métodos a utilizar son:

Método Inductivo: Este Método lo hemos utilizado para sacar conclusiones a partir del análisis de la muestra que nos conduzca a la conclusión general (proceso analítico-sintético).

Método Descriptivo: Porque hemos descrito las variables, factores, cualidades y atributos que tiene nuestra población de estudio.

Método analítico: Este Método lo utilizamos para analizar la información primaria y secundaria, y así arribar a los hallazgos y resultados, relacionados con los indicadores, dimensiones y variables que conforman la presente investigación.

3.6.2. Técnicas de recolección de datos

- **Bibliográficas:**

  Se utilizará esta técnica para recoger información secundaria, relacionada con antecedentes, marco teórico y otros aspectos de las variables objeto de estudio.

- **La encuesta:**

  Estadísticamente representativa será la técnica que se empleará para obtener información ya que tiene una gran capacidad para estandarizar datos, lo que a su vez permite su tratamiento informático y la generalización de los mismos.

Instrumentos:

- **Fichas y Formatos:**

  Se utilizó fichas resúmenes y bibliográficas, además de los formatos diseñados para recoger información primaria y secundaria de realidad del objeto de estudio.

- **Cuestionario:**

  Utilizaremos un cuestionario de 10 preguntas que estará aplicada a 45 personas (muestra).

3.7. Procedimiento para la recolección de datos

Para recolectar los datos se seguirán los siguientes pasos:

Paso 1: selección de la población y muestra, en este caso se procedió a Seleccionar los Jueces, Fiscales y abogados que serán encuestados. La aplicación del instrumento se realizará en distintos horarios y distintos días para obtener información confiable y necesaria para la investigación.

Paso 2: Elección de las técnicas e instrumentos seleccionar un programa de análisis; se empleará el programa estadístico StaticalPackageforthe Social Sciense (SPSS) y Microsoft Excel 2013 para la tabulación y obtención de tablas y gráficos como resultado de la aplicación del instrumento de recolección de datos a la muestra en estudio.

Paso 3: Verificación y tabulación de la información. Consiste en explorar los datos; luego de aplicar el instrumento a la muestra se

ejecutará el programa de análisis respectivo (SPSS 20), se exportará los datos extraídos del programa SPSS a un formato Excel para obtener los gráficos respectivos.

Paso 4: Interpretación de la información que se obtendrán de la aplicación del instrumento de recolección de datos.

Los instrumentos que se han aplicado para la recopilación de los datos han sido elaborados de acuerdo a la Operacionalización de las variables por parte de los investigadores; en ellos se reflejan los indicadores y dimensiones consideradas para la ejecución del presente estudio; muchos de ellos están basados en una escala de Likert; el recojo de esta información nos ha concedido establecer la propuesta de nuestro estudio. Los instrumentos elaborados y aplicados se consignan en los anexos de nuestro informe.

3.8. Análisis estadístico e interpretación de los datos

Se dará uso de las tecnologías científicas para los procesos de procedimientos de los datos, a través del programa Microsoft Excel.

Paso 1: Se Seleccionará un programa de análisis; se empleará el programa estadístico Microsoft Excel, para la tabulación y obtención de tablas y gráficos como resultado de la aplicación del instrumento de recolección de datos a la muestra en estudio.

Paso 2: Se explorará los datos; luego de haber aplicado el instrumento a la muestra se ejecutará el programa de análisis respectivo, se exportará los datos extraídos del programa Excel

para obtener los gráficos respectivos. Se presentará información en forma de cuadros y gráficos cuantitativos con precisiones porcentuales, ordenamiento de mayor a menor o viceversa, además se presentarán resúmenes, esquemas y diagramas.

3.9. Criterios éticos:

De los criterios citados según Belmont (1979) en su informe sobre "Principios éticos y normas para el desarrollo de investigación que involucran seres humanos" utilizaremos los siguientes:

Autonomía: Es la capacidad de las personas de deliberar sobre sus finalidades personales y de actuar bajo la dirección de las decisiones que pueda tomar. Todos los individuos deben ser tratados como seres autónomos y las personas que tienen la autonomía mermada tienen derecho a la protección.

Justicia: Equidad en la distribución de cargas y beneficios. El criterio para saber si una actuación es o no ética, desde el punto de vista de la justicia, es valorar si la actuación es equitativa. Debe ser posible para todos aquellos que la necesiten. Incluye el rechazo a la discriminación por cualquier motivo. Es también un principio de carácter público y legislado.

CAPÍTULO IV:

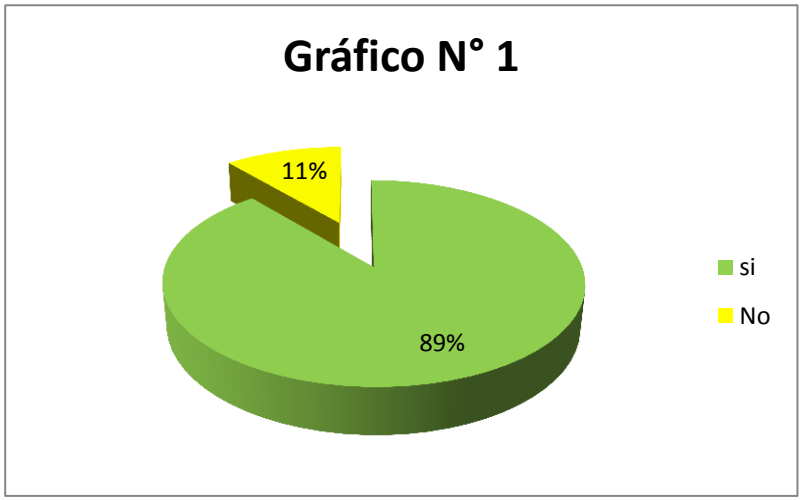
ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

IV. ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS

Figura N° 1: tipificación de los delitos informáticos.

1. ¿Conoce usted acerca de la tipificación de los delitos informáticos en la Legislación Peruana?

ALTERNATIVAS	ENC.
Si	40
No	5
TOTAL	**45**



Fuente: Elaborado por el investigadora

INTERPRETACIÓN:

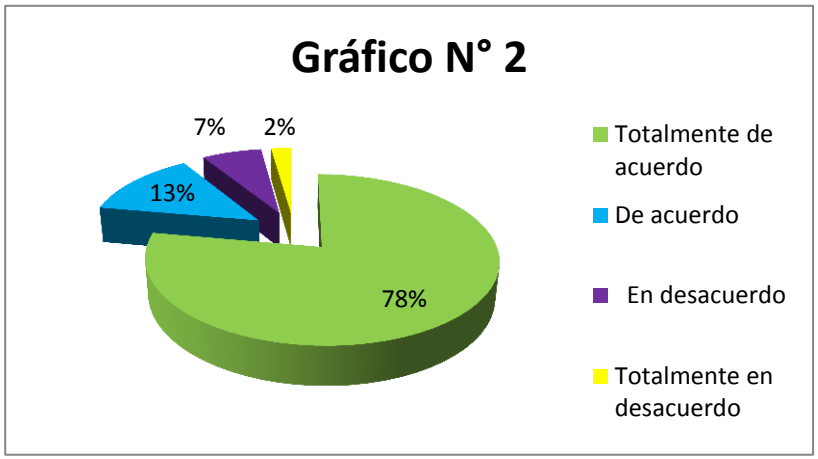
Como resultado de la investigación, se puede apreciar que un 89% de los encuestados tienen conocimiento acerca de los delitos informáticos en la Legislación Peruana teniendo un mayor porcentaje, siendo que solo el 11% considera No conocer acerca de la tipificación de los delitos informáticos.

ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS GRAFICO N° 2

Figura 2: El uso de la informática y la tecnología

¿Considera que el uso de la informática y la tecnología constituyen medios útiles y eficaces para que afecten nuevos bienes jurídicos?

ALTERNATIVAS	ENC.
Totalmente de acuerdo	35
De acuerdo	6
En desacuerdo	3
Totalmente en desacuerdo	1
TOTAL	**45**



Fuente: Elaborado por el investigador

INTERPRETACIÓN:

De acuerdo a los datos obtenidos en el grafico N° 2 se puede apreciar que el 78% están totalmente de acuerdo y el 13 % están de acuerdo que el uso de la informática y la tecnología constituyen medios útiles y eficaces para que afecten nuevos bienes jurídicos, siendo solo el 7 y 2% considera en desacuerdo.

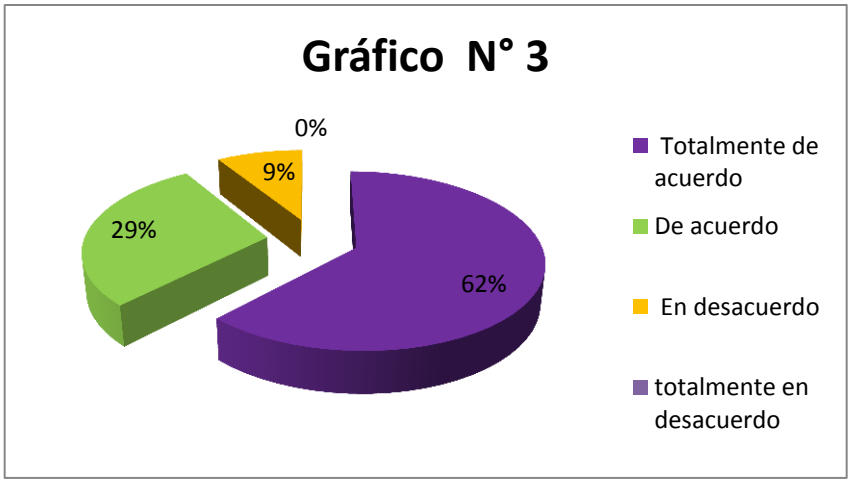
ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS GRAFICO N° 3

Figura 3: Como factor que contribuye al incremento de delitos informáticos.

¿Tiene usted en cuenta que el avance tecnológico es el mayor factor que contribuye al incremento de delitos informáticos?

ALTERNATIVAS	ENC.
Totalmente de acuerdo	28
De acuerdo	13
En desacuerdo	4
Totalmente en desacuerdo	0
TOTAL	**45**

.



Fuente: Elaborado por el investigador

INTERPRETACIÓN:

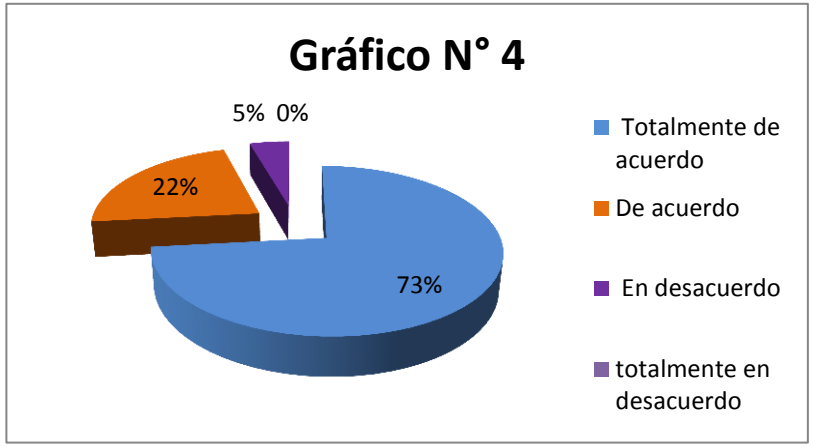
De las 45 personas encuestadas se tiene que el 62% considera Totalmente de acuerdo y con un 29% que consideraron de acuerdo, que el avance tecnológico es el mayor factor que constituye el incremento de delitos informáticos, mientras que el 9% se considera en desacuerdo.

ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS GRAFICO N° 4

Figura 4: La criminalidad informática y su regulación

¿De acuerdo a su criterio considera que la criminalidad informática en el Estado Peruano se no encuentra debidamente regulada?

ALTERNATIVAS	ENC.
Totalmente de acuerdo	33
De acuerdo	10
En desacuerdo	2
Totalmente en desacuerdo	0
TOTAL	**45**



Fuente: Elaborado por el investigador

INTERPRETACIÓN:

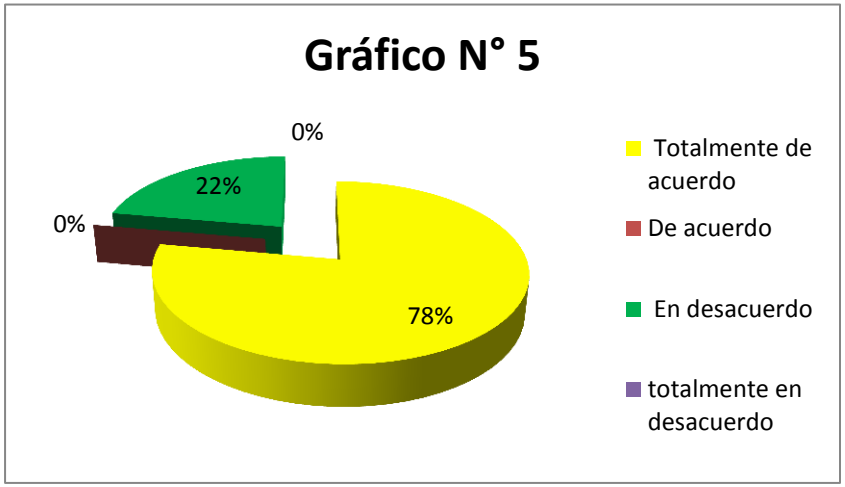
Se puede apreciar de los resultados del grafico N° 4 que de las 45 personas encuestadas el 73% considera totalmente de acuerdo y con un 22 % de acuerdo que considera que la criminalidad informática no se encuentra debidamente regulada, mientras que el 5% en desacuerdo.

ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS GRAFICO N° 5

Figura 5: el delito de atentado a la integridad de un sistema informático.

¿Considera que la Ley 30096 - ley de delitos informáticos, en su artículo N° 4, no es precisa en relación al delito de atentado a la integridad de sistemas informáticos?

ALTERNATIVAS	ENC.
Totalmente de acuerdo	35
De acuerdo	0
En desacuerdo	10
Totalmente en desacuerdo	0
TOTAL	**45**



Fuente: Elaborado por el investigador

INTERPRETACIÓN:

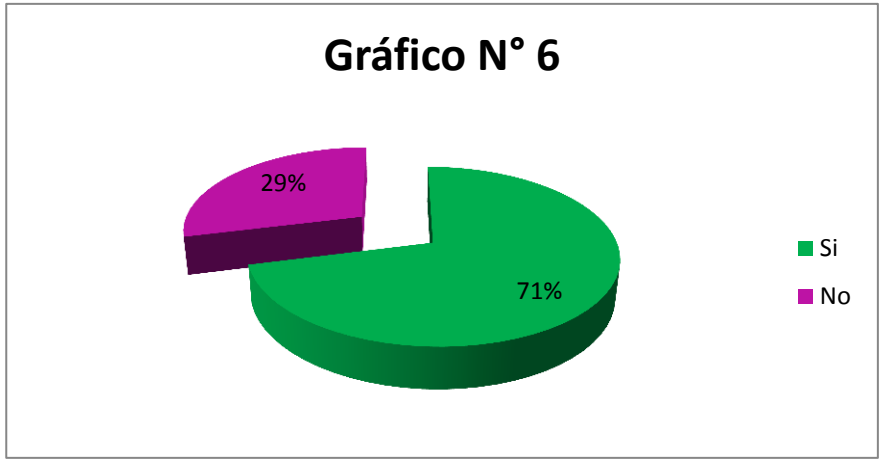
Se tiene que de las 45 personas encuestadas el 78% considera totalmente de acuerdo en que la Ley de delitos Informativos y su modificatoria no es precisa en relación al delito de atentado a la integridad de sistemas informáticos, siendo solo el 22% considera en desacuerdo.

ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS GRAFICO N° 6

Figura 6: el delito de atentado a la integridad de un sistema informático.

¿Cree usted que existe una similitud entre el delito de atentado a la integridad de sistemas informáticos tipificado en la Ley 30171 y el delito de daños tipifica en el Articulo 205 del Código Penal?

ALTERNATIVAS	ENC.
Si	32
No	13
TOTAL	**45**



Fuente: Elaborado por el investigador

INTERPRETACION:

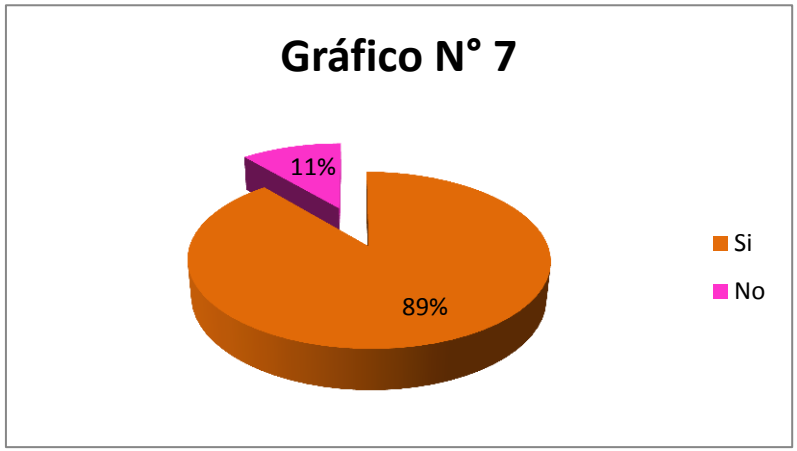
De los resultados obtenidos en el grafico N° 6, se tiene que de las 45 personas encuestadas el 71% considera que si existe una similitud entre ambos delitos y el 29% considera No.

ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS GRAFICO N° 7

Figura 7: deficiente determinación del bien jurídico

¿Considera que el delito de AISI tiene una deficiente determinación del bien jurídico protegido, situación que afecta la calificación penal y la imputación por parte del Ministerio Público?

ALTERNATIVAS	ENC.
Si	40
No	5
TOTAL	**45**



Fuente: Elaborado por el investigador

INTERPRETACIÓN:

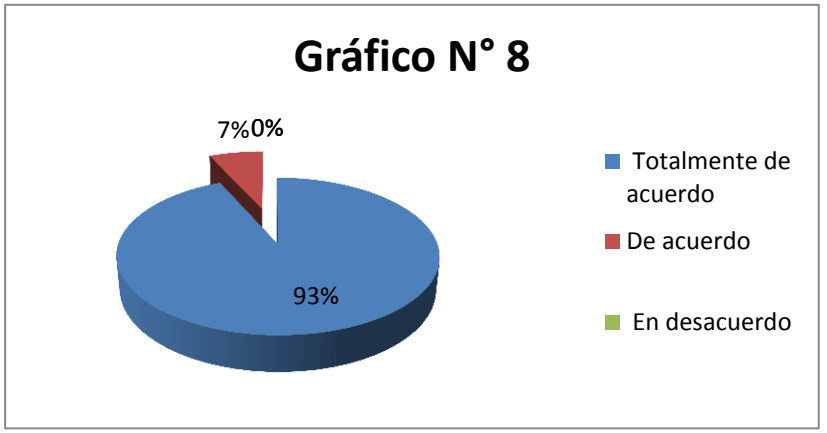
De los resultados obtenidos en el gráfico N° 7, se tiene que de las 45 personas encuestadas el 89% considera que el delito de AISI tiene una deficiente determinación del bien jurídico protegido, afectando de esa manera la imputación por parte del Ministerio Público, siendo que solo el 11% se considera en desacuerdo.

ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS GRAFICO N° 8

Figura 8: circunstancias agravantes

¿Considera que debe considerarse como circunstancia agravante cuando se afecte un sistema diseñado para brindar algún servicio público o industrial, afectando el normal abastecimiento o prestación de los servicios públicos?

ALTERNATIVAS	ENC.
Totalmente de acuerdo	42
De acuerdo	3
En desacuerdo	0
Totalmente en desacuerdo	0
TOTAL	**45**



Fuente: Elaborado por el investigador

INTERPRETACIÓN:

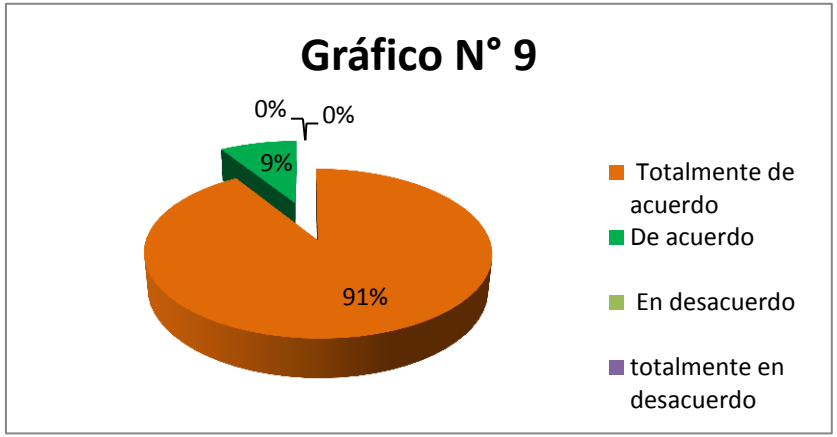
La observación del gráfico N° 8, nos permite interpretar esta conducta también debe ser sancionada, teniendo que de las 45 personas encuestadas el 93% están totalmente de acuerdo, siendo solo el 7% que está en desacuerdo.

ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS GRAFICO N° 9

Figura 9: circunstancias agravantes

¿Considera usted que debe considerarse como una circunstancia agravante cuando la comisión del delito de AISI no solo afecta al propietario sino que también afecta a terceras personas?

ALTERNATIVAS	ENC.
Totalmente de acuerdo	41
De acuerdo	4
En desacuerdo	0
Totalmente en desacuerdo	0
TOTAL	**45**



Fuente: Elaborado por el investigador

INTERPRETACION:

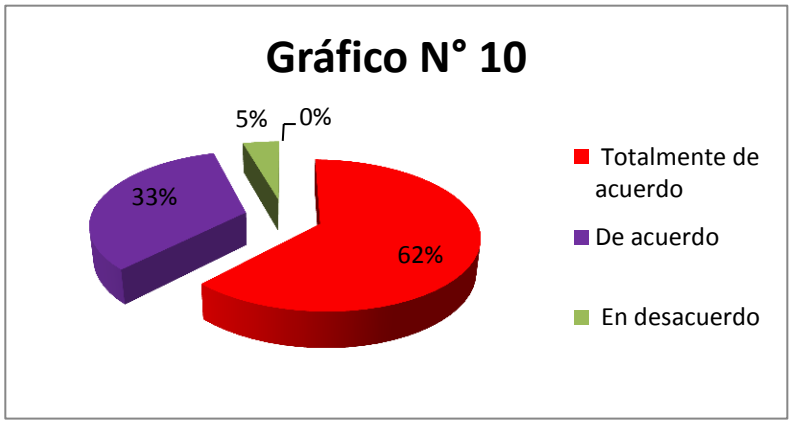
De los resultados obtenidos, se tiene que el 91% de las personas encuestadas, consideran totalmente de acuerdo y un 4 % que están de acuerdo en relación que debe considerarse como una circunstancia agravante cuando la comisión del delito de AISI no solo afecta al propietario del sistema informático si no también cuando esta afectación trasciende a terceras personas.

ANALISIS E INTERPRETACIÓN DE LOS RESULTADOS GRAFICO N° 10

Figura 10: Propuesta legislativa

¿Considera usted que es necesario una propuesta legislativa que modifique el delito de atentado a la integridad de sistemas informáticos, e incorpore circunstancias agravantes con el fin de salvaguardar los intereses de las personas y de sus sistemas informáticos?

ALTERNATIVAS	ENC.
Totalmente de acuerdo	28
De acuerdo	15
En desacuerdo	2
Totalmente en desacuerdo	0
TOTAL	**45**



INTERPRETACIÓN:

De la observación del grafico N° 10 nos permite interpretar que al criterio de las personas encuestadas consideran si es necesario una propuesta legislativa con el fin de salvaguardar los sistemas informáticos, siendo que de las 45 personas encuestadas un 62% que consideran totalmente de acuerdo y el 5% considera en desacuerdo.

4.1. Discusión

Para poder probar nuestra hipótesis general, la cual establece que de que si existen deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos entonces en ese sentido, consideramos que la norma no es clara en función al bien jurídico protegido, situación que afecta la calificación penal y la imputación por parte del Ministerio Público, en consecuencia, es recomendable la modificación del artículo N° 4 de la Ley 30096 y su modificatoria Ley N° 30171.

La LDI derogó los Arts. 207-A, 207-B y 207-C CP, reemplazando a los dos primeros por los Delitos de Acceso Ilícito (Art. 2 LDI), Atentado a la integridad de datos informáticos (Art. 3 LDI) y Atentado a la integridad de sistemas informáticos (Art. 4 LDI). Siguiendo los parámetros establecidos por el Convenio de Budapest, se puede afirmar que el bien jurídico protegido por estos tipos penales es la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. (Rueda, 2009, p. 174)

¿El delito de AISI puede ser considerado una especie del delito de daños? ¿Cuáles son los encuentros y desencuentros entre ambas figuras penales? Si consideramos que el art. 205 del CP, dentro de los delitos contra el patrimonio, al sancionar el delito de daños, reprime con una pena privativa de la libertad no mayor de tres años a “el que daña, destruye o inutiliza un bien, mueble o inmueble, total o parcialmente ajeno” y a esta norma penal la concordamos con el art. 4 de la LDI “el que […] inutiliza total o parcialmente el sistema informático”, podemos comprobar, como primera observación, que ambos tipos penales utilizan el verbo “inutilizar”.

Luego, cuando Salinas Siccha. (2013), trabaja el delito de daños, advierte que:

“inutilizar consiste en provocar la pérdida de la capacidad del bien para ejercer la función normal que le compete, sin que haya lesión en el aspecto material” (pág. 1281).

Concepto perfectamente aplicable al delito de AISI. Estas son las razones y las coincidencias por la que resulta pertinente establecer algunos lineamientos para saber cuándo estamos frente al delito de daños y cuándo frente al delito de AISI. Para ello, debemos formular algunas hipótesis provisionales de trabajo que luego vamos a desarrollar. Primero: Tanto el delito de daños (art. 205 CP) como el delito de AISI (art. 4 LDI) tienen como objeto de la acción penal a bienes muebles. Segundo: El delito de daños, a diferencia del delito de AISI, establece que el bien mueble objeto de la acción penal debe ser total o parcialmente ajeno. Tercero: El delito de daños, a diferencia del delito de AISI, establece un criterio económico para diferenciar una falta de un delito. Cuarto: Lege lata, ante un caso de daños materiales a bienes muebles, el criterio para diferenciar, el delito de AISI del delito de daños, debe atenderse a la naturaleza informática o no del bien mueble objeto material del delito. Quinto: El delito de AISI adolece de serias deficiencias en su regulación, por cuanto no ha definido el medio comisivo que lo diferencie del delito de daños común. Sexto: La pésima técnica legislativa en el delito de AISI permite incluso (sino estamos atentos) confundirlo por momentos con el delito de coacción.

El delito de atentado a la integridad de sistemas informáticos es un delito compuesto por cuanto tiene hasta cuatro verbos rectores en el siguiente orden: inutilizar, impedir, entorpecer e imposibilitar, los mismos que no son convergentes (no se requiere la concurrencia de los cuatro verbos para la configuración del ilícito penal, basta la concurrencia de uno de ellos) ni excluyentes.

Por otro lado en función a los casos suscitados en el Perú, El Juzgado Penal de Turno Permanente de la Corte Superior de Justicia de Lima

Norte, encontró responsabilidad contra la ex supervisora de procesos operativos de la agencia 2 del Centro Comercial Mega Plaza del Banco de Crédito del Perú (BCP), Katherine Flor Morales La Cruz (33), por los delitos informáticos, Contra el patrimonio, fraude informático-contra datos y sistemas informáticos, acceso ilícito, en agravio del BCP. En audiencia en una sala del Poder Judicial, la titular de la 13 Fiscalía Provincial Penal de Lima Norte, acusó, a Morales La Cruz, el haber accedido al sistema informático del banco de manera deliberada e ilegítima, vulnerando las medidas de seguridad establecidas y excediendo lo que la autorizaba como supervisora para su beneficio y el de nueve involucrados. (La Republica, 2017)

En dicho caso se puede apreciar que el bien jurídico de “seguridad y la intangibilidad de las comunicaciones e información informáticamente tratada o la seguridad de la información (o datos) que circulan en la red” no se encuentra regulada en el ordenamiento jurídico peruano, precisando que bajo un análisis del bien jurídico protegido, se puede apreciar el sistema informático, la data y los programas, tienen una naturaleza peculiar diferente a otros bienes; de esta manera, en el caso de los intangibles como los programas informáticos, estos responden a determinada inteligencia artificial, así mismo los “objetos de protección” no siempre están en poder del agraviado, pues cada vez más se confía su resguardo en “la nube” (dispositivo de almacenamiento virtual) situación que no se tiene o tenía en ningún otro bien mueble o inmueble antes conocido, siendo así, es necesario primero su clasificación y regulación del sistema informático en el art. 886 del CC donde se reconozca su calidad de bien mueble, esto a efectos que el sistema informático se encuentre amparado por el art. 205 del CC que sanciona el daño o destrucción de bienes muebles e inmuebles, siendo innecesario los tipos penales informáticos que redundan en esta protección.

Dentro de los casos más resaltantes encontramos el de la organización criminal “Los Reyes de las Detracciones” que lograron apropiarse del dinero asignado a cuentas de detracciones, tuvieron acceso a todos los servicios financieros que ofrecía el Banco de la Nación (BN) de Ferreñafe, sede donde habrían cometido los ilícitos, tanto José Vicente Romero Amoretti como Marco Martín Aragón Cornejo, ex jefe de Operaciones del BN y ex jefe de Operaciones de Gestor de Servicios, respectivamente, tenían a cargo un sistema informático (se les asignó un cajero para web) que les permitió tener acceso a todos los servicios que brinda el BN como cuentas de ahorros, detracciones, entre otras.

Sin embargo pese a que las penas han ido en aumento frente a la alza de delitos informáticos, se pude decir que dentro del Departamento de Investigación de Delitos de Alta Tecnología ha detectado que no es una, sino varias las organizaciones criminales que están tras los robos cibernéticos.

Según las denuncias reportadas ante la policía hay clientes de bancos que han sufrido el desfalco de sus cuentas con compras hechas en el extranjero, desde países como España, Argentina, Ecuador y Estados Unidos.

Pese a la normativa vigente el mayor obstáculo para la Policía es el acceso a las bases de datos de las entidades bancarias, necesario para rastrear el IP de la computadora de donde se realizó la ilegal transacción o transferencia de dinero.

Las entidades financieras se amparan en la Ley del Secreto Bancario, para no proporcionar información a los investigadores. De acuerdo al artículo 143 de la Ley General del Sistema Financiero y del Sistema de Seguros (Ley general), las solicitudes de levantamiento de secreto bancario podrán ser presentadas a las entidades bancarias o a la SBS solo por los jueces y tribunales, por el fiscal de la Nación y por el

presidente de una comisión investigadora del Congreso, en casos específicos.

Asimismo la Policía tiene un limitado acceso a las cámaras de video de las agencias financieras o cajeros donde se registraron presuntamente los ilícitos denunciados por los clientes. La autorización para visualizar las imágenes incluso llegan después de un mes de denunciado el ilícito, en muchos casos esos videos han sido borrados.

La Policía requiere como máximo 4 días para poder efectivizar sus investigaciones con el rastreo del IP, incluso si el cliente advierte el fraude en las primeras 24 horas (flagrancia) se podría evitar la trasferencia de dinero a la cuenta del delincuente y su identificación.

CAPITULO V

PROPUESTA LEGISLATIVA

V. PROPUESTA DE INVESTIGACIÓN

PROPUESTA LEGISLATIVA:

TÍTULO DEL PROYECTO DE LEY: LEY QUE MODIFICA EL ARTICULO N° 4 DE LA LEY 30096 – LEY DE DELITOS INFORMATICOS.

EXPOSICIÓN DE MOTIVOS:

En el Perú, la LDI, en su art. 4, regula el delito denominado “atentado a la integridad de sistemas informáticos” (en adelante AISI). Sin embargo, tal como pretendemos demostrar en el presente artículo, producto de una pésima técnica legislativa, el legislador peruano, al no tener claro el objeto de la acción sobre el cual recaen los cuatro verbos rectores utilizados en el tipo penal, confunde por ratos, el AISI con los delitos de daños y, en otros momentos, con el delito de coacción. Perdiendo de vista, por lo tanto, el bien jurídico protegido y la naturaleza propia de este delito que forma parte del cibercrimen y, en consecuencia, de una nueva manifestación de la criminalidad.

La situación se agrava cuando, pese a encontrar su inspiración en el Convenio sobre Cibercriminalidad de Budapest 2001, el legislador no regula, tal como este lo establece, el modus operandi o el medio comisivo a utilizarse por el agente, perjudicando con ello el propósito de lograr establecer y definir de manera idónea el contenido o contorno preciso de la conducta penalmente relevante en este tipo penal.

El delito de atentado a la integridad de sistemas informáticos, nomen juris adoptado por nuestra legislación en la Ley de Delitos Informáticos, es conocido dentro de otras legislaciones como sabotaje o daño informático, el cual, forma parte de una gama de delitos que tienen en común el uso de las tecnologías de la información y comunicación para su comisión.

El Código Penal, hasta antes de la promulgación de la LDI, el 22 de octubre del 2013, regulaba dentro del Título V “De los delitos contra el patrimonio”, en el Capítulo X, lo que denominaba “delitos informáticos”. Así, el antecedente inmediato y directo del tipo penal en comento es el derogado art. 207-B del CP, el cual expresamente reprimía lo siguiente:

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

Como podemos advertir, de la lectura del derogado art. 207-B del CP, se regulaba dentro de un mismo tipo penal a dos delitos que a la fecha son independientes uno del otro en la LDI. El primero, el delito de atentado a la integridad de datos informáticos, contemplado en el art. 3; el segundo, el delito de AISI contemplado en el art. 4 del mismo cuerpo normativo.

Ya hemos establecido el antecedente nacional del AISI. Entonces, ¿cuál es el antecedente internacional? Al respecto, podemos señalar que el legislador, en este tema, ha seguido las pautas establecidas en el convenio, el cual, luego de establecer en su artículo primero las definiciones de “datos” y “sistemas informáticos” (recogidas íntegramente por nuestra legislación) procede en su art. 4 a señalar los lineamientos que cada Estado Parte debe regular en su legislación interna para reprimir el AISI, entendiendo por esta a “[…] la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos”.

Concepto perfectamente aplicable al delito de AISI. Estas son las razones y las coincidencias por la que resulta pertinente establecer algunos lineamientos para saber cuándo estamos frente al delito de daños y cuándo frente al delito de AISI. Para ello, debemos formular algunas hipótesis provisionales de trabajo que luego vamos a desarrollar. Primero: Tanto el delito de daños (art. 205 CP) como el delito

de AISI (art. 4 LDI) tienen como objeto de la acción penal a bienes muebles. Segundo: El delito de daños, a diferencia del delito de AISI, establece que el bien mueble objeto de la acción penal debe ser total o parcialmente ajeno. Tercero: El delito de daños, a diferencia del delito de AISI, establece un criterio económico para diferenciar una falta de un delito. Cuarto: Lege lata, ante un caso de daños materiales a bienes muebles, el criterio para diferenciar, el delito de AISI del delito de daños, debe atenderse a la naturaleza informática o no del bien mueble objeto material del delito. Quinto: El delito de AISI adolece de serias deficiencias en su regulación, por cuanto no ha definido el medio comisivo que lo diferencie del delito de daños común. Sexto: La pésima técnica legislativa en el delito de AISI permite incluso (sino estamos atentos) confundirlo por momentos con el delito de coacción.

Dicho lo anterior, vamos a desarrollar una interpretación del AISI de lege lata. Luego vamos a trabajar sus falencias, vacíos y omisiones. Finalmente vamos a proponer una lege ferenda.

El delito de atentado a la integridad de sistemas informáticos es un delito compuesto por cuanto tiene hasta cuatro verbos rectores en el siguiente orden: inutilizar, impedir, entorpecer e imposibilitar, los mismos que no son convergentes (no se requiere la concurrencia de los cuatro verbos para la configuración del ilícito penal, basta la concurrencia de uno de ellos) ni excluyentes.

Además, debe agregarse que en algunos casos se afecta el normal abastecimiento o prestación de los servicios públicos, la seguridad nacional, etc. Más adelante, agregan los autores españoles, un enfoque desde la trasnochada concepción jurídica económica resulta a la fecha insuficiente, razón por la que debe trabajarse desde una perspectiva funcional que comprenda tanto la integridad como la disponibilidad de la información contenida en redes o soportes informáticos (concepto funcional de propiedad y patrimonio), entendiéndose que se afecta “la posibilidad de disponer en todo momento, de modo íntegro y con plena funcionalidad operativa, de los datos, programas y sistemas con los que

operamos en nuestra vida, privada o pública, diaria" (DE LA MATA Y HERNADEZ, 2009, pág. 33).

En el caso del Perú, atendiendo a la concreta tipificación establecida en el art. 4 de la LDI, podemos señalar que el bien jurídico protegido es la integridad, el acceso y la funcionabilidad o prestación de sus servicios del sistema informático. Resulta obvio que además de bienes específicamente propios del delito informático, se afecta el patrimonio del titular del sistema informático afectado. Más adelante analizaremos las falencias de la tipificación.

Respecto del bien jurídico protegido en los delitos informáticos, ya hemos sostenido que la doctrina internacional no es pacífica. De la Mata y Hernández, efectuando un excelente resumen respecto de la postura de reconocidos autores, sostienen que, en los delitos informáticos, lo que se protege es: la información y la accesibilidad a la información; la accesibilidad y la integridad de la información y de los sistemas informáticos; simplemente la información; la seguridad de los sistemas informáticos, entendida como el derecho a no sufrir injerencias externas en los datos, programas o sistemas informáticos, por la trascendencia que estos tienen para el desarrollo mundial; la comunicación pacífica a través de las redes telemáticas, con independencia, se dirá, de las garantías y protección que pueden ofrecerse a otros bienes jurídicos como la intimidad o la protección a datos de carácter personal; la confianza en el funcionamiento de los sistemas informatizados, como interés de carácter supraindividual, de los que dependen todas las actividades tanto públicas como privadas; o incluso, directamente, la tecnología de Internet, bien jurídico, se dirá, de primera magnitud (DE LA MATA BARRANCO Y HERNÁNDEZ DÍAZ, 2009, pág. 328).

ANÁLISIS COSTO BENEFICIO

El presente proyecto de ley, no origina ni demanda gasto alguno para el Estado, por el contrario, busca la protección de los sistemas informáticos, permitiendo de esta forma salvaguardar los derechos fundamentales de las personas ante cualquier conducta que atente a la integridad de sus sistemas informáticos

TEXTO NORMATIVO:

PROYECTO DE LEY

Los congresistas de la Republica, en función que suscriben, ejerciendo el derecho de iniciativa legislativa que les confiere el artículo 107 de la Constitución Política del Perú, presentan el proyecto de ley:

FORMULA LEGAL:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la siguiente Ley:

LEY QUE MODIFICA EL ARTICULO N° 4 DE LA LEY 30096 – LEY DE DELITOS INFORMATICOS.

1. **Articulo 1.- Modificación del artículo 4 de la Ley 30096, Ley de delitos informáticos.**

   Artículo 4: atentado a la integridad de sistemas informáticos

   El que por cualquier medio y de manera deliberada e ilegítima inutiliza, total o parcialmente, un sistema informático, impide el acceso de este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

   El Juez aumentará la pena privativa de libertad hasta en un tercio por encima del máximo legal en los siguientes casos:

- Cuando el daño trasciende los ámbitos de dominio del propietario y causen un grave perjuicio en agravio de terceros.

- Cuando se afecte un sistema diseñado para brindar algún servicio público o industrial, afectando el normal abastecimiento o prestación de los servicios públicos.

DISPOCISIONES COMPLEMENTARIAS

Primera: Adecuación de normas

La presente ley se adecuara a la normativa nacional, en un plazo no mayor de 60 días calendarios.

Segundo: Vigencia

La presente ley entrara en vigencia al día siguiente de su publicación.

Comuníquese al Señor Presidente de la Republica para su promulgación.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

VI. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Con el uso de la tecnología han surgido diferentes modalidades delictivas, las cuales no están muy bien reguladas por el ordenamiento jurídico peruano, es por ello que el Estado en el año 2013 promulga la Ley 30096 – Ley de Delitos Informáticos, sin embargo esta no regula de manera precisa el delito de atentado a la integridad de sistemas informáticos, por lo que se debe modificar el artículo 4 de dicha ley, incorporando no solo a los medios tecnológicos de información y comunicación sino también a los medios tradicionales como medios comisivos de este delito; con el objetivo de salvaguardar los intereses de las personas, de sus sistemas informáticos.

2. Además, debe considerarse en este tipo penal circunstancias agravantes, esto es cuando en algunos casos se afecta el normal abastecimiento o prestación de los servicios públicos, la seguridad nacional, y, cuando el daño trasciende los ámbitos de dominio del propietario y causen un grave perjuicio en agravio de terceros, ya que estas son circunstancias que tienen mayor responsabilidad penal y deben ser sancionadas con una mayor pena.

3. El legislador debe establecer criterios de valoración económica o una escala de valoración de gravedad de los daños ocasionados tanto al sistema informático como de los efectos y consecuencias que acarrean a partir del referido daño.

RECOMENDACIONES

1. Se recomienda que el delito informático de AISI sea modificado, debido a que es un delito que no se agota solo en la afectación al patrimonio, sino que, muchas veces, por efecto de los daños ocasionados al sistema informático, el perjuicio se extiende más allá adquiriendo la naturaleza de un delito pluriofensivo. Por otro lado se protege son intereses de contenido económico, los cuales no deben identificarse con el patrimonio en sentido estricto, por cuanto en un delito de esta naturaleza, “las consecuencias económicas principales y más graves no se limitan a la de la pérdida del valor económico de los datos afectados, sino que se expanden al perjuicio para, por ejemplo, la actividad empresarial que se esté llevando a cabo.

2. Además, debe agregarse que en algunos casos se afecta el normal abastecimiento o prestación de los servicios públicos, la seguridad nacional, etc. Más adelante, agregan los autores españoles, un enfoque desde la trasnochada concepción jurídica económica resulta a la fecha insuficiente, razón por la que debe trabajarse desde una perspectiva funcional que comprenda tanto la integridad como la disponibilidad de la información contenida en redes o soportes informáticos (concepto funcional de propiedad y patrimonio), entendiéndose que se afecta “la posibilidad de disponer en todo momento, de modo íntegro y con plena funcionalidad operativa, de los datos, programas y sistemas con los que operamos en nuestra vida, privada o pública, diaria”.

3. Debemos señalar que el delito en comento es un delito compuesto por cuanto tiene hasta cuatro verbos rectores en el siguiente orden: inutilizar, impedir, entorpecer e imposibilitar, los mismos que no son convergentes (no se requiere la concurrencia de los cuatro verbos para la configuración del ilícito penal, basta la concurrencia de uno de ellos). Sin embargo, cabe anotar que tampoco son excluyentes, por cuanto el agente de manera

deliberada e ilegítima puede comenzar por entorpecer, para luego impedir, siendo que finalmente decide imposibilitar o inutilizar el acceso, el funcionamiento o la prestación de servicios de determinado sistema informático.

REFERENCIAS BIBLIOGRAFICAS

Aboso, G y Zapata, M. (2006). Cibercriminalidad y derecho penal, Buenos Aires-Montevideo: B de F.

Bramont Arias Torres, Luis Alberto y María del Carmen GarciasCantizano. (1998). Manual de derecho penal. Parte especial, 4.a ed., Lima, Perú: Editorial San Marcos.

Bramont Arias Torres, Luis Alberto. (2000). El delito informático. Lima, Perú: Actualidad Jurídica.

Bramont Arias Torres, L (2010). Código Procesal Penal, Lima, Perú, Gaceta Penal & Procesal Penal.

Caro Coria, Dino Carlos, (2006). Problemas de interpretación judicial en los delitos contra la libertad e indemnidad sexuales, en el portal web de Caro & Asociados, Lima, Perú. Recuperado de <bit.ly/2dVi39B>.

De la Mata, N y Hernández L. (2009). El delito de daños informáticos: una tipificación defectuosa", en Estudios Penales y Criminológicos, n.° 29, Santiago de Compostela: Recuperado de <bit.ly/2mfabS3>.

DoigDiaz, Y. (2006). El Proceso de Terminación Anticipada en el Código Procesal Penal de 2004. Lima, Perú, Actualidad Juridica.

Durand Valladares, Raúl. (2002). Los delitos informáticos en el Código Penal peruano. Lima, Perú: Revista Peruana de Ciencias Penales

Fondo de las Naciones Unidas para la Infancia, Grooming. (2014). Guía práctica para adultos. Información y consejos para entender y prevenir el acoso a través de Internet. Lima, Perú: Recuperado de <uni. cf/2gdSUcK>.

Galgano, F. (2005). La globalización en el espejo del derecho, Buenos Aires: Rubinzal-Culzoni.

García Cantizano, María del Carmen. (2000). La delincuencia informática en el ordenamiento jurídico peruano. Lima, Perú: Actualidad Juridica.

García Cantizano, María del Carmen. (1994). Falsedades documentales, Valencia, España: Tirant lo Blanch.

Gantes, Bill. (1999). Me path to the future, Nueva York, EEUU: Avon Books.

Gestion, Digiware. (2016). Seis sectores están en la mira de los ataques cibernéticos, en el portal web del diario Gestión, Lima, Perú. Recuperado de <bit. ly/1MRuZU4>.

Gutierrez, M. (1994). InformationTechnology. Computer Crime and Other Crimes against Information Technology in Spain, en Sieber, Ulrich (ed.), Information Technology crime.National legislations and international initiatives, Colonia: Carl Heymans.

Gutiérrez, M. (1994). Notas sobre la delincuencia informática: atentados contra la 'información' como valor económico de empresa", en Arroyo Zapatero, Luis y Klaus Tiedemann (eds.), Estudios de derecho penal económico y de la empresa, Cuenca, Ecuador: Ediciones de la Universidad de Castilla-La Mancha.

Gonzáles, J. (1999). Protección penal de sistemas, elementos, datos, documentos y programas informáticos en el derecho español", n.° 01-14, Granada. Recuperado de <bit.ly/2mf86FB>.

Montero, J. (2014). Introducción al Derecho Jurisdiccional Peruano. Lima, Perú. Editorial Estrella.

Orts, E. y Roig, M. (2001). Delitos informáticos y delitos comunes cometidos a través de la informática, Valencia: Tirant lo Blanch.

Pérez, A. (1996). Manual de informática y derecho, Barcelona: Ariel.

Picotti, L. (2006). Internet y derecho penal: un empujón únicamente tecnológico a la armonización internacional, en Romeo Casabona, Carlos María (coord.), El cibercrimen: nuevos retos jurídicos-penales, nuevas respuestas político-criminales, Granada: Comares.

Rodríguez, C. (2003). Criminalidad y sistemas informáticos, en Diego Díaz-Santos, María Rosario y Eduardo A. Fabián Caparrós (coords.), El sistema penal frente a los retos de la nueva sociedad, Madrid: Colex.

Romeo, C. (2006). De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal, en Romeo Casabona, Carlos María (coord.), El cibercrimen: nuevos retos jurídicos-penales, nuevas respuestas político-criminales, Granada: Comares.

Rosas, J. (2009). Derecho Procesal Penal con aplicación al Nuevo Proceso Penal DEC. Leg. N° 957, Lima, Perú, Jurista Editores.

Salinas, R. (2013). Derecho penal. Parte especial, 5.a ed., Lima: Grijley.

Salvadori, I. (2013). La regulación de los daños informáticos en el Código Penal italiano", en Revista de Internet, Derecho y Política, n.° 16, Barcelona: Recuperado de <bit.ly/2mTzgW2>.

San Martin, C (2015). Derecho Procesal Penal Lecciones. Lima, Perú, Instituto Peruano de Criminología y Ciencias Penal y Centro de Altos Estudios de Ciencias Jurídicas, políticas y sociales.

Taboada, G. (2001). El proceso especial de terminación anticipada en el nuevo Código procesal penal. Especial referencia a su aplicación al distrito judicial de La Libertad. Lima, Perú, Jurista Editores.

Taboada, G. (2009). El proceso especial de terminación anticipada en el nuevo Código procesal Penal. Especial referencia a su aplicación en el distrito Judicial de La Libertad. Lima, Perú, Gaceta Penal & Procesal Penal. Tomo 2

Villavicencio, T. (2014). Felipe, Delitos informáticos en la Ley N.° 30096 y la modificación de la Ley N.° 30171, en Revista Virtual del Centro de Estudios en Derecho Penal, n.° 1, Lima: Recuperado de <bit.ly/2fDeUtb>.

Velásquez, P. (2009). La Determinación de la Pena en el Proceso de Terminación Anticipada. Lima, Perú, Gaceta Penal & Procesal Penal. Tomo 5.

ANEXOS

ANEXO I – ENCUESTA

1. ¿Conoce usted acerca de nueva tipificación de los delitos informáticos en la Legislación Peruana?

    a) Si
    b) No

2. Considera que el uso de la informática y la tecnología constituyen medios útiles y eficaces para que afecten nuevos bienes jurídicos?

    a) Totalmente de acuerdo
    b) De acuerdo
    c) En desacuerdo
    d) Totalmente en desacuerdo

3. ¿Tiene usted en cuenta que el avance tecnológico es el mayor factor que contribuye al incremento de delitos informáticos?

    a) Totalmente de acuerdo
    b) De acuerdo
    c) En desacuerdo
    d) Totalmente en desacuerdo

4. ¿De acuerdo a su criterio considera que la criminalidad informática en el Estado Peruano se no encuentra debidamente regulada?

    a) Totalmente de acuerdo
    b) De acuerdo
    c) En desacuerdo
    d) Totalmente en desacuerdo

5. ¿Considera que la Ley 30096 - ley de delitos informáticos, en su artículo N° 4, no es precisa en relación al delito de atentado a la integridad de sistemas informáticos??

    a) Totalmente de acuerdo
    b) De acuerdo
    c) En desacuerdo
    d) Totalmente en desacuerdo

6. ¿Cree usted que existe una similitud entre el delito de atentado a la integridad de sistemas informáticos tipificado en la Ley 30171 y el delito de daños tipifica en el Articulo 205 del Código Penal?

    a) Si
    b) No

7. ¿Considera que el delito de AISI tiene una deficiente determinación del bien jurídico protegido, situación que afecta la calificación penal y la imputación por parte del Ministerio Público?

    a) Si
    b) No

8. ¿Considera que debe considerarse como circunstancia agravante cuando se afecte un sistema diseñado para brindar algún servicio público o industrial, afectando el normal abastecimiento o prestación de los servicios públicos?

    a) Totalmente de acuerdo
    b) De acuerdo

c) En desacuerdo
d) Totalmente en desacuerdo

9. ¿Considera usted que debe considerarse como una circunstancia agravante cuando la comisión del delito de AISI no solo afecta al propietario sino que también afecta a terceras personas?

a) Totalmente de acuerdo
b) De acuerdo
c) En desacuerdo
d) Totalmente en desacuerdo

10. ¿Considera usted que es necesario una propuesta legislativa que modifique el delito de atentado a la integridad de sistemas informáticos, e incorpore circunstancias agravantes con el fin de salvaguardar los intereses de las personas y de sus sistemas informáticos??

a) Totalmente de acuerdo
b) De acuerdo
c) En desacuerdo
d) Totalmente en desacuerdo

ANEXO II

Ley de Delitos Informáticos

LEY Nº 30096

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República

Ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY DE DELITOS INFORMÁTICOS

CAPÍTULO I

FINALIDAD Y OBJETO DE LA LEY

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

CAPÍTULO II

DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

“Artículo 2. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.**”**

“Artículo 3. Atentado a la integridad de datos informáticos

El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.**”**

(*) Artículo modificado por el Artículo 1 de la Ley Nº 30171, publicada el 10 marzo 2014

Artículo 4. Atentado contra la integridad de sistemas informáticos

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.**”**

(*) Artículo modificado por el Artículo 1 de la Ley Nº 30171, publicada el 10 marzo 2014**,**

CAPÍTULO III

DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. **(*)**

(*) Artículo modificado por el Artículo 1 de la Ley Nº 30171, publicada el 10 marzo 2014**, cuyo texto es el siguiente:**

“Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.**"**

CAPÍTULO IV

DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Artículo 6. Tráfico ilegal de datos

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

(*) Artículo derogado por la Única Disposición Complementaria Derogatoria de la Ley Nº 30171, publicada el 10 marzo 2014**.**

Artículo 7. Interceptación de datos informáticos

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

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

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales. **(*)**

(*) Artículo modificado por el Artículo 1 de la Ley Nº 30171, publicada el 10 marzo 2014**, cuyo texto es el siguiente:**

“Artículo 7. Interceptación de datos informáticos

El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.**”**

CAPÍTULO V

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 8. Fraude informático

El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social. **(*)**

(*) Artículo modificado por el Artículo 1 de la Ley Nº 30171, publicada el 10 marzo 2014**, cuyo texto es el siguiente:**

“Artículo 8. Fraude informático

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o

manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.**”**

CAPÍTULO VI

DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

Artículo 9. Suplantación de identidad

El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

CAPÍTULO VII

DISPOSICIONES COMUNES

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. **(*)**

(*) Artículo modificado por el Artículo 1 de la Ley Nº 30171, publicada el 10 marzo 2014**, cuyo texto es el siguiente:**

“Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.**”**

Artículo 11. Agravantes

El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.

2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.

4. El delito compromete la defensa, la seguridad y la soberanía nacionales.

"Artículo 12. Exención de responsabilidad penal

Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos.**" (*)**

(*) Artículo incorporado por el Artículo 3 de la Ley Nº 30171, publicada el 10 marzo 2014**.**

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA. Codificación de la pornografía infantil

La Policía Nacional del Perú puede mantener en sus archivos, con la autorización y supervisión respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento de datos informáticos, para fines exclusivos del cumplimiento de su función. Para tal efecto, cuenta con una base de datos debidamente codificada.

La Policía Nacional del Perú y el Ministerio Público establecen protocolos de coordinación en el plazo de treinta días a fin de cumplir con la disposición establecida en el párrafo anterior.

SEGUNDA. Agente encubierto en delitos informáticos

El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se

cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

TERCERA. Coordinación interinstitucional de la Policía Nacional del Perú con el Ministerio Público

La Policía Nacional del Perú fortalece al órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, la Policía Nacional del Perú centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad. **(*)**

(*) Disposición modificada por el Artículo 2 de la Ley Nº 30171, publicada el 10 marzo 2014**, cuyo texto es el siguiente:**

"TERCERA. Coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados

La Policía Nacional del Perú fortalece el órgano especializado encargado de coordinar las funciones de investigación con el Ministerio Público. A fin de establecer mecanismos de comunicación con los órganos de gobierno del Ministerio Público, el centro de respuesta temprana del gobierno para ataques cibernéticos (Pe-CERT), la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y los Organismos Especializados de las Fuerzas Armadas, la Policía Nacional centraliza la información aportando su experiencia en la elaboración de los programas y acciones para la adecuada persecución de los delitos informáticos, y desarrolla programas de protección y seguridad.**"**

CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reforzada en el plazo de treinta días desde la vigencia de la presente Ley. **(*)**

(*) Disposición modificada por el Artículo 2 de la Ley Nº 30171, publicada el 10 marzo 2014**, cuyo texto es el siguiente:**

"CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de comunicaciones y demás actividades correspondientes para dar efectividad a la presente Ley, la Policía Nacional del Perú, el Ministerio Público, el Poder Judicial, el Pe-CERT (Centro de respuesta temprana del gobierno para ataques cibernéticos), la ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), Organismos Especializados de las Fuerzas Armadas y los operadores del sector privado involucrados en la lucha contra los delitos informáticos deben establecer protocolos de cooperación operativa reformada en el plazo de treinta días desde la vigencia de la presente Ley.**"**

QUINTA. Capacitación

Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal -especialmente de la Policía Nacional del Perú, el Ministerio Público y el Poder Judicial- en el tratamiento de los delitos previstos en la presente Ley.

SEXTA. Medidas de seguridad

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) promueve permanentemente, en coordinación con las instituciones del sector público, el fortalecimiento de sus medidas de seguridad para la protección de los datos informáticos sensibles y la integridad de sus sistemas informáticos.

SÉTIMA. Buenas prácticas

El Estado peruano realiza acciones conjuntas con otros Estados a fin de poner en marcha acciones y medidas concretas destinadas a combatir el fenómeno de los ataques masivos contra las infraestructuras informáticas y establece los mecanismos de prevención necesarios, incluyendo respuestas coordinadas e intercambio de información y buenas prácticas.

OCTAVA. Convenios multilaterales

El Estado peruano promueve la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de los delitos informáticos.

NOVENA. Terminología

Para efectos de la presente Ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001:

a. **Por sistema informático:** todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

b. **Por datos informáticos:** toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

DÉCIMA. Regulación e imposición de multas por la Superintendencia de Banca, Seguros y AFP

La Superintendencia de Banca, Seguros y AFP establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 5 del artículo 235 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente.

UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece la escala de multas atendiendo a las características, complejidad y circunstancias de los casos aplicables a las empresas bajo su supervisión que incumplan con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por el Decreto Legislativo 957.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa, con los recaudos correspondientes sobre las características, complejidad y circunstancias del caso particular, a fin de aplicarse la multa correspondiente. **(*)**

(*) Disposición modificada por el Artículo 2 de la Ley Nº 30171, publicada el 10 marzo 2014**, cuyo texto es el siguiente:**

"UNDÉCIMA. Regulación e imposición de multas por el Organismo Supervisor de Inversión Privada en Telecomunicaciones

El Organismo Supervisor de Inversión Privada en Telecomunicaciones establece las multas aplicables a las empresas bajo su supervisión que incumplan

con la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal, aprobado por Decreto Legislativo 957.

Las empresas de telecomunicaciones organizan sus recursos humanos y logísticos a fin de cumplir con la debida diligencia y sin dilación la obligación prevista en el numeral 4 del artículo 230 del Código Procesal Penal.

El juez, en el término de setenta y dos horas, pone en conocimiento del órgano supervisor la omisión incurrida por la empresa a fin de que el Organismo Supervisor de Inversión Privada en Telecomunicaciones aplique la multa correspondiente.**”**

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

PRIMERA. Modificación de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional

Modifícase el artículo 1 de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, modificado por el Decreto Legislativo 991 y por Ley 30077, en los siguientes términos: (*) RECTIFICADO POR FE DE ERRATAS

“**Artículo 1. Marco y finalidad**

La presente Ley tiene por finalidad desarrollar legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional.

Solo podrá hacerse uso de la facultad prevista en la presente Ley en los siguientes delitos:

1. Secuestro.

2. Trata de personas.

3. Pornografía infantil.

4. Robo agravado.

5. Extorsión.

6. Tráfico ilícito de drogas.

7. Tráfico ilícito de migrantes.

8. Delitos contra la humanidad.

9. Atentados contra la seguridad nacional y traición a la patria.

10. Peculado.

11. Corrupción de funcionarios.

12. Terrorismo.

13. Delitos tributarios y aduaneros.

14. Lavado de activos.

15. Delitos informáticos."

SEGUNDA. Modificación de la Ley 30077, Ley contra el crimen organizado

Modifícase el numeral 9 del artículo 3 de la Ley 30077, Ley contra el crimen organizado, en los siguientes términos:

"**Artículo 3. Delitos comprendidos**

La presente Ley es aplicable a los siguientes delitos

9. Delitos informáticos previstos en la ley penal." **(*)**

(*) Confrontar con el Artículo 4 del Decreto Legislativo Nº 1244, publicado el 29 octubre 2016.

TERCERA. Modificación del Código Procesal Penal

Modifícase el numeral 4 del artículo 230, el numeral 5 del artículo 235 y el literal a) del numeral 1 del artículo 473 del Código Procesal Penal, aprobado por Decreto Legislativo 957 y modificado por Ley 30077, en los siguientes términos: (*) RECTIFICADO POR FE DE ERRATAS

"**Artículo 230. Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación**

(...)

4. Los concesionarios de servicios públicos de telecomunicaciones deberán facilitar, en el plazo máximo de treinta días hábiles, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones, así como la información sobre la identidad de los titulares del servicio, los números

de registro del cliente, de la línea telefónica y del equipo, del tráfico de llamadas y los números de protocolo de internet, que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las veinticuatro horas de los trescientos sesenta y cinco días del año, bajo apercibimiento de ser pasible de las responsabilidades de ley en caso de incumplimiento. Los servidores de las indicadas empresas deberán guardar secreto acerca de las mismas, salvo que se les citare como testigos al procedimiento. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos o software, se encontrarán obligados a mantener la compatibilidad con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. **(*)**

(*) Confrontar con el Artículo 6 de la Ley Nº 30171, publicada el 10 marzo 2014**.**

Artículo 235. Levantamiento del secreto bancario

5. Las empresas o entidades requeridas con la orden judicial deberán proporcionar, en el plazo máximo de treinta días hábiles, la información correspondiente o las actas y documentos, incluso su original, si así se ordena, y todo otro vínculo al proceso que determine por razón de su actividad, bajo apercibimiento de las responsabilidades establecidas en la ley. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

Artículo 473. Ámbito del proceso y competencia

1. Los delitos que pueden ser objeto de acuerdo, sin perjuicio de los que establezca la Ley, son los siguientes:

a) Asociación ilícita, terrorismo, lavado de activos, delitos informáticos, contra la humanidad;" **(*)**

(*) Confrontar con el Artículo 2 del Decreto Legislativo Nº 1301, publicado el 30 diciembre 2016**, el mismo que entró en vigencia a nivel nacional a los noventa (90) días contados a partir del día siguiente de su publicación en el Diario Oficial El Peruano.**

CUARTA. Modificación de los artículos 162, 183-A y 323 del Código Penal

Modifícanse los artículos 162, 183-A y 323 del Código Penal, aprobado por el Decreto Legislativo 635, en los siguientes términos:

"**Artículo 162. Interferencia telefónica**

El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

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

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales. **(*)**

(*) Confrontar con el Artículo 4 de la Ley Nº 30171, publicada el 10 marzo 2014**.**

Artículo 183-A. Pornografía infantil

El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.

La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando:

1. El menor tenga menos de catorce años de edad.

2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173 o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de doce ni mayor de quince años. De ser el caso, el agente será inhabilitado conforme a los numerales 1, 2 y 4 del artículo 36.

Artículo 323. Discriminación

El que, por sí o mediante terceros, discrimina a una o más personas o grupo de personas, o incita o promueve en forma pública actos discriminatorios, por motivo racial, religioso, sexual, de factor genético, filiación, edad, discapacidad, idioma, identidad étnica y cultural, indumentaria, opinión política o de cualquier índole, o condición económica, con el objeto de anular o menoscabar el reconocimiento, goce o ejercicio de los derechos de la persona, será reprimido con pena privativa de libertad no menor de dos años ni mayor de tres o con prestación de servicios a la comunidad de sesenta a ciento veinte jornadas.

Si el agente es funcionario o servidor público, la pena será no menor de dos ni mayor de cuatro años e inhabilitación conforme al numeral 2 del artículo 36.

La misma pena privativa de libertad señalada en el párrafo anterior se impondrá si la discriminación se ha materializado mediante actos de violencia física o mental, o si se realiza a través de las tecnologías de la información o de la comunicación." **(*)**

(*) Confrontar con el Artículo 4 de la Ley Nº 30171, publicada el 10 marzo 2014**.**

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria

Deróganse el numeral 4 del segundo párrafo del artículo 186 y los artículos 207-A, 207-B, 207-C y 207-D del Código Penal. (*) RECTIFICADO POR FE DE ERRATAS