UNIVERSIDAD SAN PEDRO

FACULTAD DE DERECHO Y CIENCIAS POLÍTICA

ESCUELA DE DERECHO

El Derecho Informático aplicado al Derecho Penal en el Perú

2019

Trabajo de suficiencia profesional para obtener el título

profesional de Abogado

Autor

Huaney Bayona Edwin Vidal

Asesor

Diaz Ambrosio Silverio,

Huaraz-Perú

2019

DEDICATORIA

A mis Padres y una persona especial, porque creyeron mi y porque me sacaron adelante, dándome, ejemplos dignos de superación, porque en gran parte gracias a ustedes, hoy puedo ver alcanzada mi meta, ya que siempre estuvieron impulsándome en los momentos más difíciles de mi carrera, y porque el orgullo que sienten por mí, fue lo que me hizo ir hasta el final.

AGRADECIMIENTO

Gracias a Dios por haber puesto en mi camino a aquellas personas que me acompañaron durante todo el periodo de estudio y por permitirme haber llegado hasta este momento tan importante de mi formación profesional.

Para mis maestros por la motivación para la culminación de mis estudios profesionales.
A todos, espero no defraudar los y contar siempre con su valioso apoyo, sincero e incondicional.

PRESENTACIÓN

Señores miembros del jurado

En cumplimiento a las disposiciones legales del reglamento de Grados y Títulos de la Facultad de Derecho y Ciencias Políticas de la Universidad San Pedro, tengo a bien a someter a vuestra consideración el presente trabajo de Suficiencia Profesional titulado:

" el derecho informático aplicado al derecho penal en el Perú " con el fin de optar el título de Abogado.

El presente trabajo es desarrollado en la ciudad de Huaraz desempeñándome como asistente jurídico con el grado de Bachiller en el estudio Jurídico de Hermógenes Luna Valverde, con Registro C.A.A. N°2076 “Abogados Asociados “.
Aprovecho la ocasión, para expresar mi agradecimiento a los docentes de la facultad de Derecho y Ciencias Políticas, que con su experiencia y conocimientos han contribuido a mi formación profesional

Edwin Vidal Huaney Bayona
BA. Derecho

Palabras - clave

Tema	**Derecho, Penal, Informático**
Especialidad	**Derecho Informático**

Keywords:

Text	**Law, Criminal, Computer**
Specialty	**Computer Law**

Línea de Investigación: Derecho

INDICE GENERAL

INTRODUCCION

El fenómeno informático es una realidad incuestionable e irreversible; definitivamente, la informática ha instalado entre nosotros para no marcharse jamás. Ello es consecuencia del continuo y progresivo desarrollo del campo de la informática aplicada en la actualidad a todos los aspectos de la vida cotidiana; así, por ejemplo, la utilización de computadoras en la industria, el comercio, la administración pública, en instituciones bancarias y financieras.

Ésta verdadera invasión de la computadora en todo los ámbitos de las relaciones socioeconómicas, ha motivado que muchos hablen de una auténtica "era informática".

En efecto, pocas dimensiones de nuestra vida no se ven afectadas, dirigidas o controladas por la computadora, ya sea de manera directa o indirecta; incluso en determinados casos, las computadoras no solo son utilizadas como medios de archivo o procesamiento de información, sino que, además se les concede la capacidad de adoptar automáticamente decisiones.

"Derecho Informático aplicado al Derecho Penal en el Perú", título de esta monografía, es sin lugar a dudas un tema relativamente nuevo, no solo en esta parte del mundo; sin embargo ya hay países que se han puesto a la vanguardia, aunque con algunas diferencias creadas por estudiosos y profesionales de la materia, pero es inevitable el control legal.

¿Quién no ha tenido un virus (un ejemplo, simple del perjuicio que causa un programa hecho, mal intencionado) en su computadora?, este problema es el que motivó a la realización de este trabajo monográfico, para saber hasta dónde pueden llegar, en su límite jurídicamente y poder combatir a estas personas., si bien es cierto que la tecnología avanza a pasos agigantados en el mundo, se ve creciendo un temor

enorme por el control de este fenómeno, que nos invade, en todos los ámbitos de nuestras vidas, los delitos informáticos, causados por gente (como los Hacker, cracker, phreaking, carding, o sus diversas modalidades) con mediano o alto grado de conocimiento de esta tecnología.

El objetivo de esta trabajo de suficiencia profesional es dar conocer algunos de los diferentes tipos de Delitos Informáticos. No pretendo hacer de esta monografía un compendio de las leyes Peruanas o de otros países, pero si se hará alguna mención de legislaciones que se van dando en el tiempo progresivamente en el Perú, en el Capítulo I y II, Derecho Informático, veremos aspectos referentes al tema que nos ayuden a entender esta materia de estudio; el Capítulo III, y siguientes trataremos la implicancia del derecho informático al derecho penal en cuanto a los delitos informáticos.

CAPITULO I

ANTECEDENTES:

1.1.-Antecedentes bibliográficos

a nivel nacional tenemos los siguientes estudios:

Arata Salinas, Ángel Alfonso 2002. Titulo : Comercio electrónico - Derecho y legislación Perú Internet - Derecho y legislación - Perú Tecnología de la información en el Perú la toma de conciencia sobre el desarrollo de la nueva rama del Derecho, denominado Derecho Informático, nace como consecuencia de la aparición de la computadora, la misma que hace posible el acopio, uso, manipulación y transmisión de la información por medios de soportes electrónicos y redes que cada día son más sofisticadas y de uso masivo por la población, siendo una parte activa de todo ello el comercio, por lo que resulta de mayor importancia tratar el tema del comercio electrónico y por su relevancia en el medio ha generado todo un universo comercial en un mundo paralelo al mundo real conocido como mundo virtual o ciberespacio, materia de estudio del Derecho Informático de difícil comprensión, al entender de la mayoría de estudiosos del derecho. Ante esta realidad, el objetivo del presente trabajo es describir, precisar, esclarecer y analizar la nueva problemática que se viene planteando en la comercialización de bienes y servicios, a través de medios electrónicos, al estarse desarrollándose nuevas instituciones que contienen

nuevas ideas y conceptos con respecto al comercio globalizado, donde el Derecho Civil debe partir de la codificación del espacio, tiempo y las cosas que conllevan nuevos conceptos del comercio, haciéndolos más seguros y confiables a través de las redes abiertas de comunicación que se viene dando y que regirá en el futuro no muy lejano en la sociedad y el Derecho. La metodología del presente trabajo es descriptiva y empírica, partiendo de la descripción del desarrollo de la sociedad de la información, del desarrollo de tecnologías para el comercio electrónico, de las implicancias jurídicas en el comercio electrónico, los alcances de la legislación comparada, donde se describen los nuevos elementos que se vienen dando en el Derecho Informático con respecto al comercio electrónico, desde la aparición de la computadora hace cuatro décadas, dividiéndose el presente trabajo en cuatro capítulos. El Primer Capítulo trata sobre la tecnología de la información y el derecho, partiendo de la convergencia de la informática con las telecomunicaciones, desde la aparición de la computadora como herramienta del desarrollo del hombre, su versatilidad y convergencia con las telecomunicaciones, al permitirle el manejo de abundante información, globalizando al mundo mediante redes cerradas y abiertas, influyendo al cambio de las relaciones humanas, las mismas que por su importancia son materia de regulación jurídica en la sociedad actual. El Segundo Capítulo aborda el comercio electrónico y su trascendencia jurídica, trata sobre los soportes informáticos utilizados en el comercio electrónico, su naturaleza virtual, originando nuevos conceptos de orden jurídico con relación al tiempo y espacio y el uso de los soportes técnicos para la ejecución de las transacciones virtuales de bienes y servicios materiales e incorpóreo existentes. El Tercer Capítulo; es el tema de los aspectos jurídicos de los documentos electrónicos, desarrolla el nuevo concepto del tema documento al existir nuevas formas de representarse como su incorporeidad o inmaterialidad del mismo; replanteando dichos conceptos, por tratarse de nuevos actos fragmentarios, dinámicos y de constante evolución que pasarán a ser parte del acervo jurídico del presente y futuro.

EL Cuarto Capítulo; y último trata sobre los alcances de la legislación peruana y comparada sobre comercio electrónico. Por ser nuestro país receptor de tecnologías

no se ha desarrollado una legislación específica sobre el comercio electrónico, abordándose la legislación comparada como fuente de inspiración para la regulación en un futuro del comercio electrónico, tal como se desprenden de los proyectos y propuestas planteadas por los estudiosos del Derecho informático, como reto y respuesta a esta sociedad de la información de la que somos parte.

Espinoza Espinoza, Juan 1999 , Título : Resultado

La tutela jurídica del tratamiento de los datos personales frente a los avances de la informática. Sobre el denominado "derecho general de la personalidad

Delpiazzo, Carlos 2011, Título : Resultado

La convergencia tecnológica (de la Informática y las Telecomunicaciones) y la convergencia jurídica (de los Derechos administrativos impuesta por la globalización) han aparejado sensibles transformaciones en el campo de la contratación pública. Partiendo de la consideración de los acuerdos alcanzados en materia a nivel de la Organización Mundial del Comercio (OMC), de la Unión Europea (UE) y del Mercado Común del Sur (MERCOSUR), el trabajo examina cómo se ha evolucionado hacia la regulación de la contratación pública por medios electrónicos en Europa y América Latina.

Alva Manchego, Fernando Emilio,2009, Título: Resultado

Actualmente, el plagio de documentos digitales es un problema que afecta, en diferentes dimensiones, a la sociedad en su conjunto y, muy especialmente, al ámbito académico. Conociendo las graves consecuencias que puede traer su expansión, se decide realizar un trabajo que consiste en la implementación de un sistema de información que permita la detección automática de plagio en documento en formato electrónico. Se incurre en plagio cuando se indica que una persona es autora de "algo" (ideas plasmadas en documentos) que en realidad no ha elaborado y que ha copiado de 4otra persona o fuente sin realizar alguna modificación sustancial o un aporte personal y sin referenciar convenientemente a la autora original.

Gonzales Villa, Tania Denisse,2013, Título : Resultado

En el Perú, la inseguridad ciudadana, en general, sigue siendo uno de los grandes motivos de temor para la población. Este problema se ha ido incrementando a través de los años por diversos factores como el desempleo, la falta de valores en la sociedad, una mala calidad de educación, escasez de los recursos con los que cuentan las entidades responsables para combatir este inconveniente, entre otros. Las comisarías cuentan con diversos procesos que sostienen los diferentes servicios que brindan a la comunidad. Estos procesos tales como registro de denuncias, información y gestión de trámites personales, difusión a la comunidad de un mapa de delitos, entre otros, suelen ser en su mayoría manuales, lentos y con información desactualizada. Los factores mencionados impiden a las comisarías brindar un buen servicio a la comunidad y no cumplir con salvaguardar la seguridad ciudadana. Además, se identificó la carencia de un medio de comunicación rápido y en tiempo real entre las comisarías y la comunidad. La solución propuesta consiste en un sistema Web y un sistema Móvil, los cuales permitan dar soporte informático a la gestión de los servicios que brinda una comisaría y proporcionar información para la seguridad de los ciudadanos. La memoria descriptiva cuenta con 7 capítulos que presentan la organización del proyecto de tesis.

En el capítulo 1 se describe el problema que se desea resolver, los objetivos, resultados, métodos y procedimientos, las tecnologías utilizadas, el plan de proyecto y la sustentación de la solución propuesta.

En el capítulo 2 se describe el marco conceptual de la solución planteada y el estado del arte donde se exponen ejemplos que resuelven parte del problema en la actualidad. En el capítulo 3 se describen los requisitos funcionales y se desarrolla el análisis de la solución que consiste en explicar la viabilidad del sistema en términos técnicos y de costo, y se identifican el diagrama de clases inicial que constituye una base para el trabajo posterior. En el capítulo 4 se describe la arquitectura seleccionada para cumplir con los requisitos planteados del sistema, además se presenta también en este capítulo el diseño de la interfaz gráfica de la aplicación,

definiendo los criterios para la selección del diseño y las principales pantallas de la aplicación con sus respectivas características.

En el capítulo 5 se detalla cómo se ha aplicado la tecnología seleccionada en la solución del problema. En el capítulo 6 se presentan las observación.

Villavicencio Terreros, Felipe, 2014 , Título: Resultado

En los últimos tiempos, debido al desarrollo de la tecnología de la información, se ha desarrollado una nueva forma de delito llamada delitos informativos. En relación con este nuevo tipo de delito, se emitió una ley penal especial, cuyo propósito es prevenir y sancionar las actividades ilegales que afectan sistemas informáticos y datos, comunicaciones secretas y otros bienes legales que se ven afectados con este tipo de delito, como la equidad , fe pública y libertad sexual.

Chang O´Campo, Katherine, 2000, Título: Resultado

Desde antigua data, la correspondencia epistolar fue el medio de comunicación utilizado para contratar por aquellas personas entre las cuales no era posible una comunicación inmediata; Con los adelantos de la ciencia, la contratación se ha venido realizando a través de otros medios, tales como el teléfono o el telegrama. Hoy en día, los individuos emplean a los medios informáticos como nuevos sistemas de comunicación para celebrar los más variados negocios jurídicos. Esto último no es sino prueba de la influencia de la informática sobre el Derecho, la misma que puede ser analizada desde múltiples perspectivas. Por ejemplo, si abordamos el tema desde la óptica del derecho penal, hablaremos de un delito informático. Si analizamos la materia desde el arista del derecho industrial, hablaremos del dominio de campos en internet o de la Resolución N°21- 1998/0DA-INDECOPI, publicada el17 de julio del año de 1998 que regula el uso del software o programa de ordenador. El presente trabajo, sin embargo, abordará el tema desde una perspectiva distinta, pues nuestro propósito es que el lector advierta las modalidades que presenta la contratación electrónica, así como la problemática existente al respecto. Ahora bien, la contratación electrónica comprende dos grandes campos. De un lado, encontramos a los contratos informáticos y de otro, a los contratos telemáticos.

CAPITULO II

MARCO TEÓRICO

2.1.- El derecho informático y el derecho penal

El derecho informático abarca las ciencias jurídicas que se encarga de observar el comportamiento en el ámbito informático que afecte a la sociedad.; por eso se necesita una correcta implementación y regularlos adecuadamente

En el derecho penal se afronta un reto en cuanto la sanción y clasificación de los delitos, ya que el delito se define como una conducta que es sancionada por las leyes de defensa social. No obstante, debido a su novedad, el derecho aún no prevé muchos actos informáticos ilegales como delitos o el castigo por la misma causa.

2.2.- Definición del tema

Derecho Informático se define como un conjunto de principios y normas que reguilan los efectos jurídicos. Es una rama del derecho especializado en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales. “ El Derecho Informático es la aplicación del derecho a la informática permitiendo que se adopten o creen soluciones jurídicas a los problemas que surgen en torno al fenómeno informático.

Tal es la problemática generada por este fenómeno que ha motivado en la actualidad la necesidad de recurrir al Derecho Penal a fin de disuadir del uso abusivo al que lleva el empleo de computadoras, lo cual se ha plasmado ya en varias legislaciones extranjeras. No obstante, ante estas situaciones no puede olvidarse el principio del Derecho Penal como *ultima ratio*, según el cual la intervención penal sólo está justificada cuando otras ramas del Ordenamiento jurídico ya no pueden resolver los problemas que genera el fenómeno informático en la sociedad, de ahí que el Derecho Penal actúe como última instancia de control social.

2.3.- Fundamentación del tema

Realidad problemática

Todas las actividades del hombre están regidas por el Derecho. Desde antes de su nacimiento, en el momento de la concepción, está protegido por la ley. Y cuando muere, sus decisiones tienen trascendencia más allá de su existencia, a través de los derechos y obligaciones que hereda a sus sucesores. Pensemos en cualquier actividad externa del hombre y veremos que está regida por el Derecho. Por supuesto, en esta época de avances Tecnológicos, la informática, la telemática, la cibernética, la computación y los sistemas no son materias ajenas a la ciencia jurídica. El uso de cajeros automáticos, las compras por Internet, el navegar por la red, la contratación para acceder a Internet, el Chat, la pornografía infantil en línea, la piratería de programas, la piratería de la información, los fraudes bancarios, los derechos de Autor sobre material publicado en Internet, el uso de tarjetas de crédito en terminales, las declaraciones patrimoniales de los servidores públicos, los casinos en red, el correo electrónico, y la contaminación y destrucción de información que se encuentra en equipos de cómputo (mediante el envío de virus), son algunas de las actividades y eventos regulados por el Derecho Informático o donde la Informática se aplica al Derecho.

Es en esa línea de análisis, que el impresionante e incontenible progreso de las comunicaciones, demanda de la comunidad jurídica la adecuación de sus ordenamientos jurídicos para hacer frente a las diversas manifestaciones de la informática expresadas a través del uso de la Internet, del procesamiento de datos a través de sistemas digitales, el empleo de Software especializados; etc., que no son sino herramientas útiles que sin una correcta regulación podrían ser utilizadas por manos inescrupulosas para cometer actos ilícitos, de ahí que toda esta corriente de vanguardia denominada como la *revolución informática*, debe ser ampliamente estudiada, sobre todo en las aulas universitarias.

2.4.- El derecho informático

En este capítulo se hará un estudio del Derecho Informático, sus alcances, y la irradiación que tiene en la actualidad sobre el Derecho Penal; para así tener un mayor acercamiento a nuestra realidad y a su vez a la problemática social que nos avoca.

2.5.- Surgimiento del derecho informático

Los conceptos de tecnología y sociedad de información son antecedentes necesarios del derecho informático, con la finalidad de regular el comportamiento en un ámbito tecnológico. Desde la aparición de la **computación** como un fenómeno, ésta ha sido benéfica en las distintas áreas de la ciencia y la cultura. Sin embargo, la aparición de actos delictivos a través de la informática ha devenido en la creación de esta rama del derecho. Desde la aparición de la **computación** como un fenómeno**,** ésta ha sido benéfica en las distintas áreas de la ciencia y la cultura. Sin embargo la aparición de actos delictivos a través de la informática ha devenido en la creación de esta rama de derecho.

2.6.- Formas de vinculación de la ciencia jurídica

- El derecho informático abarca las ciencias jurídicas que se encarga de observar el comportamiento en el ámbito informática que afecte a la sociedad; por eso se necesita una correcta implementación y regularlos adecuadamente.
- La informática legal es el estudio y análisis jurídico que la ciencia jurídica debe realizar para su aplicación correcta, y esto se define como el conjunto de técnicas destinadas al tratamiento lógico.
- La informática jurídica existe para modernizar el derecho según la forma en que avance la tecnología.

2.7.- Campos de estudio

- Acceso a la información
- Administración de justicia y nuevas tecnologías
- Banca y dinero digital
- Censura en internet. Libertad de expresión online
- Comercio Electrónico
- Contratos Informáticos
- Correo electrónico
- Defensa del consumidor
- Delitos Informáticos
- Derecho de las Telecomunicaciones
- Derecho Laboral e Informática. Teletrabajo.
- Documento Electrónico, mensajes de datos, EDI y Factura Electrónica
- Editoriales online de derecho
- Firma Electrónica
- Hábeas data
- Impuestos e internet
- Informática Jurídica

- Informática Legal
- Manifestación de la Voluntad por Medios Electrónicos
- Medidas Cautelares sobre Equipos Informáticos
- Nombres de Dominio y Direcciones IP
- Notificación por Medios Electrónicos
- Protección de datos
- Propiedad Intelectual y Propiedad Industrial e Internet
- Programas: software jurídico. Bases de datos y Gestión de Bufetes
- Protección de Datos de Carácter Personal
- Publicidad e Internet
- Relación entre el derecho y la informática
- Seguridad informática
- Sociedad civil e internet
- Sociedad de la información
- Software libre
- Telefonía y Voz sobreVOIP
- Wireless ApplicationPrototocol (WAP)

2.8.- Marco conceptual

Para empezar, hay que tener en claro algunos términos del título del tema.

a) **La informática.-** Es la ciencia aplicada que abarca el estudio y aplicación del tratamiento automático de la información, utilizando dispositivos electrónicos y sistemas computacionales. También está definida como el procesamiento automático de la información, “La informática entendida como la ciencia del tratamiento automático de la información, con las posibilidades que ofrece de almacenamiento y tratamiento de la documentación y la recuperación de la información registrada en soportes

magnéticos, ópticos, u otros, permite controlar esa información y puede llegar a convertirse en un instrumento de presión y control, social."

La informática no está ajeno al derecho, aunque en algunas ocasiones parezca

estarlo y por ello en las relaciones sociales y económicas generadas como consecuencia del desarrollo e introducción en todas las áreas y actividades.

b) **Relación del derecho informático y la informática jurídica.-**constituye el conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática. Es una ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora. Es decir que la relación que existe entre estas dos ciencias es que la informática en general desde este punto de vista es objeto regulado por el derecho.

c) **Derecho informático.-** El Derecho Informático, ha sido analizado desde diversas perspectivas. Por un lado el Derecho Informático se define como un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática. Por otro lado hay definiciones que establecen que es una rama del derecho especializado en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales.

Se considera que el Derecho Informático es un punto de inflexión del Derecho, puesto que todas las áreas del derecho se han visto afectadas por la aparición de la denominada Sociedad de la Información, cambiando de este modo los procesos sociales y, por tanto, los procesos políticos y jurídicos. Es aquí donde hace su aparición el derecho informático, no tanto como una rama sino como un cambio.

d) **La informática jurídica. -** Informática jurídica es el procesamiento automático de información jurídica. Aplicación de la tecnología de la

información al derecho. Es por ende el tratamiento automatizado de las fuentes del conocimiento jurídico (sistemas de documentación legislativa, jurisprudencial y doctrinal), de las fuentes de producción jurídica.

Es una disciplina de las ciencias de la información que tiene por objeto la aplicación de la informática en el derecho. Difiere entonces del derecho informático, que es la regulación jurídica de las nuevas tecnologías.

Se pueden apreciar dos tipos de interrelaciones, **si se toma como enfoque el aspecto netamente instrumental,** se está haciendo referencia a la informática jurídica. **Pero al considerar informática como objeto del derecho, se hace alusión al Derecho de la Informática.**

Entonces podemos decir que la Informática Jurídica es la aplicación de técnicas informáticas a la documentación jurídica en los aspectos sobre análisis, archivo y recuperación de información contenida en la legislación, jurisprudencia, doctrina o cualquier otro documento; Ahora bien, con los avances tecnológicos que se han dado en la actualidad, como es el caso de los instrumentos digitales, que nos permiten accesar a la información de una manera rápida y sencilla, se nos abren puertas para mezclar estos instrumentos y expandir de modo más simple esa información.

El problema surge en el momento que los derechos de los creadores de las obras se ven violentados, debido a que con las nuevas tecnologías facilitan la transmisión de dichas obras sin el consentimiento del autor, y en muchas ocasiones con un afán de lucro, lo cual afecta el derecho patrimonial del autor, de los herederos y de los adquirientes por cualquier título. Es por eso que es importante crear normas en las cuales se contemple la forma en que se registrarán las publicaciones; los permisos autorizaciones que se deban solicitar; los medios para hacerlo, y ante qué autoridad deberán realizarse, los delitos en que se puede incurrir, y las sanciones aplicables.

Los aspectos jurídicos de internet como por ejemplo la protección de los datos personales, los derechos de autor, la contratación electrónica, los nombres de dominio, la firma digital, el tele trabajo, los delitos informáticos, requieren abogados cada vez más preparados y especializados en Derecho Informático.

e) Base de datos.- es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

f) Cracker.- Para las acciones nocivas existe la más contundente expresión, **"Cracker"** o **"Rompedor"**, sus acciones pueden ir desde simples destrucciones, como el borrado de información, hasta el robo de información sensible que se puede vender; es decir, presenta dos vertientes, el que se cuela en un sistema informático y roba información o produce destrozos en el mismo, que se dedica a desproteger todo tipo de programas, tanto de versiones Shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anti copia.

g) Denegación de servicio.- impedir una comunicación, una respuesta, causar un repudio de usuarios.

h) Hacker.- Es quien intercepta dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en computadoras pertenecientes a entidades públicas o privadas.

i) Manipulación de datos.- alteración o eliminación de la información.

j) Phreaker.- Persona que ingresa al sistema telefónico, teniendo o no equipo de computación, con el propósito de apoderarse , interferir, dañar, destruir, conocer, difundir, hacer actos de sabotaje, o hacer uso de la información

accediendo al sistema telefónico, provocando las adulteraciones, que en forma directa, conlleva este accionar, con consecuente perjuicio económico.

k) **Pirata informático.-** Es aquella persona que copia, reproduce, vende, entrega un programa de software que no le pertenece o que no tiene licencia de uso, a pesar de que el programa está correctamente registrado como propiedad intelectual en su país de origen o en otro país, esta persona adultera su estructura, su procedimiento de instalación, copiándola directamente y reproduciendo por cualquier medio la documentación que acompaña al mismo programa.

l) **Repetición.-** capturar una información, guardarla un tiempo y volverla a enviar, produciendo un efecto de no autorización.

m) **Virucker.-** Esta palabra proviene de los términos Virus y Hacker, y se refiere al creador de un programa el cual insertado en forma dolosa en un sistema de cómputo destruya, altere, dañe o inutilice a un sistema de información perteneciente a organizaciones con o sin fines de lucro y de diversa índole.

2.9.- Características del derecho informático

Naturaleza jurídica del derecho informático

Según Edgar Salazar Cano, la naturaleza jurídica del Derecho Informático radica en sus tres características esenciales

a) Que no se encuentra sectorizado o ubicado en una sola actividad, sino que es amplio y general, debido a que la informática se aplica en numerosos sectores de la actividad socioeconómica.
b) Que su unidad viene dada por la originalidad técnica impuesta por el fenómeno informático.

c) Que es un derecho complejo porque los aspectos técnicos de la informática en su interrelación con el Derecho, recaen sobre diversas ramas o especialidades jurídicas.

Este carácter interdisciplinario que presenta como rasgo esencial el Derecho de la Informática ha suscitado un debate entre quienes sustentan que se trataría de un sector de normas dispersas de diferentes disciplinas jurídicas , y quienes creemos que constituye un conjunto unitario de normas dirigidas a regular un objeto determinado, desde una metodología propia, es decir, que gozaría de autonomía.

Creemos que no le resta al Derecho de las Tecnologías de la Información su carácter de disciplina independiente el hecho de que maneje materiales suministrados por las otras ramas del Derecho, ya que lo único determinante es que debe sistematizar y reducir a unidad la pluralidad de elementos relacionados con el impacto social del fenómeno informático, de modo de presentar así un sistema orgánico y unitario que los comprenda a todos; quizás sea más difícil apreciar tal autonomía en países con un discreto desarrollo tecnológico, pero sin duda que, en los más industrializados, la informática a penetrado de tal manera en la vida social influyendo en el desarrollo socio-económico de los pueblos, que el Derecho de las tecnologías de la información sustenta bases conceptuales claras y con fundamento científico. Obviamente, el desarrollo tecnológico es determinante para el surgimiento de esta nueva rama en una sociedad, ya que en la medida en que se vaya incorporando en las labores de las personas, en el trabajo, en la forma de comunicarse, el manejo de la información a través de los sistemas informáticos hará surgir la necesidad en ese grupo social de regulación de conductas nuevas formándose una nueva rama autónoma.

En este caso, el desarrollo de las tecnologías de la información y las comunicaciones, es una fuente material del Derecho, en la medida en que el uso de esta tecnología vaya generando conductas nuevas, que deban ser recogidas y reguladas por el Derecho, y haya necesidad de hacerlo.

2.10.- Objetivos del derecho informático

El objeto de estudio del Derecho Informático es propio, aunque por el momento no necesariamente exclusivo. Esto se debe a que muchos de los aspectos abarcados por el Derecho Informático son abordados hoy en día por el derecho Penal, Civil y Comercial, debido a la falta de legislación específica que ataque las diversas problemáticas resultantes y que contemple las particularidades que la Sociedad de la Información implica. Es decir, la falta de plena autonomía en su objeto obedece más a la falta de legislación específica que a la ausencia de autonomía. Un reciente caso, que es abordado desde el derecho privado, plantea el conflicto entre el derecho del titular de una red social (Facebook) a mantener al usuario en la misma luego de que la persona física que lo había creado hubiese fallecido. La aproximación a este conflicto de intereses desde las áreas tradicionales de Derecho adolece de limitaciones para abarcar el caso en toda su extensión, ya que carece de los elementos conceptuales específicos para enmarcar adecuadamente el conflicto de intereses entre la persona jurídica propietaria de la red social y los herederos del causante. Es evidente que solo una legislación específica que contemple las particularidades de éste y otros casos similares, es absolutamente necesaria; y en los hechos varios países han estado en los últimos años legislando al respecto.

El Derecho Informático tiene dos objetivos:

a) Objetivo Inmediato.- la Informática
b) Objetivo u Objeto Mediático.- La información

2.11 El derecho informático aplicado al derecho penal

Aspectos Generales.

Los usos y costumbres sociales se han visto afectados por este desarrollo vertiginoso de las tecnologías de la información originándose situaciones jurídicas nuevas que la legislación no ha previsto**;** estando a que la información en esta nueva sociedady económica informática cumple un papel fundamental en tanto el ciudadano, la empresa privada o entidad pública que no obtenga la información necesaria para desarrollarse en sus actividades sociales y económicas para realizar sus funciones , no podrá acondicionarse a la nueva sociedad y económica de la información; no podrá participar de las ventajas y oportunidades que brinda el estar oportunamente informados; desmejorando su calidad de vida o su función.

Sucede que las personas en su vida cotidiana generan diferentes datos o información como sus viajes al interior o exterior, el uso de las tarjetas de crédito, movimientos de cuentas bancarias, declaraciones juradas ante instituciones públicas, solicitudes de ingreso o de trabajo ante instituciones públicas o privadas, los que ordenados y sistematizados por la computadora permiten obtener un perfil de comportamiento de la persona que vulnera la intimidad y la libertad de los individuos.

Debemos de sostener firmemente, que el derecho a la información asimismo se constituye en garantía de una futura decisión libre y certera; lo que conlleva a una persona libre y autónoma, que a su vez se relaciona con la facultad que debe tener la persona sobre los datos generados o proporcionados en su vida privada cotidiana entre personas, instituciones públicas o entidades privadas: con lo cual se concibe la permanente relación y conflicto entre el derecho a la informática y la intimidad que exigen una regulación legal para proteger la libertad y la intimidad de las personas.

La regulación del desarrollo de la informática en su relación con la vida privada o intimidad de las personas se centra en el reconocimiento del derecho a la información

como derecho fundamental del sistema democrático es necesario para el desarrollo individual y de la sociedad y el derecho a la intimidad como derecho base para el libre desarrollo de la personalidad; con lo cual ambos derechos se basan en la libertad y dignidad de los seres humanos; debiéndose buscar el necesario equilibrio que debe existir entre el derecho a la información y la intimidad de las personas; al ser derechos reconocidos constitucionalmente y consagrados por pactos internacionales de Derechos Humanos, como el Pacto internacional de Derechos civiles y políticos y la Convención Americana de Derechos Humanos, suscritos debidamente por el Perú.

En el esfuerzo de buscar el equilibrio entre el derecho a la información a través de la informática y el derecho a la intimidad de las personas, el ordenamiento constitucional peruano, con la Constitución de 1993, se ha creado la Garantía Constitucional (proceso constitucional) de Habeas Data que protege la libertad de las personas, cuando se vea amenazada o vulnerada por datos o información recogida, almacenada, sistematizada o trasmitida por medios informáticos o no, públicos o privados; que en buena cuenta cautela el derecho de las personas a no ser perjudicado por suministrarse información contenida en bases de datos o archivos sin su autorización.

Como se advierte de todo el razonamiento presentado, el hombre necesita de un espacio en el que pueda desenvolverse física, psíquica, afectiva, moral, amical y socialmente. Este espacio no se da solamente en el interior de su hogar sino, que se extiende a otros lugares, tales como la oficina, el despacho, el club, etcétera, viene a ser esa esfera de nuestras vidas que se conoce como privada, o sea todo aquello que sin ser secreto debe ser respetado por nuestros semejantes y el Estado, a fin de que quede libre de toda publicidad.

Es que, solo la persona natural goza del derecho a la vida privada, toda vez que no es atributo de la persona jurídica que disfruta del derecho a la confidencialidad de naturaleza diferente, al derecho a la intimidad se encuentra seriamente amenazado

por la creciente capacidad que posee tanto el sector público como el privado de acumular y acceder a gran cantidad y variedad de información; la utilización de redes imperceptibles en las que circulan a gran velocidad, a bajo costo y sin ningún tipo de control información personal; importa la creación de una sociedad en la que todos nuestros actos y datos personales quedan registrados y son eventualmente comercializados.

Para concluir este apartado, debemos de recordar que la informática no es solo un fenómeno tecnológico con implicaciones estrictamente positivas. Los ordenadores, al permitir un manejo rápido y eficiente de grandes volúmenes de información, facilitan la concentración automática de datos referidos a las personas, constituyéndose así en un verdadero factor de poder.

2.12.-Trascendencia jurídica del derecho informático en el derecho penal

El fenómeno informático ante el Derecho Penal.

El fenómeno informático es una realidad incuestionable e irreversible; definitivamente, la informática se ha cimentado entre nosotros para no apartarse fácilmente. Ello es consecuencia del continuo y progresivo desarrollo del campo de la informática aplicada en la actualidad a todos los aspectos de la vida cotidiana; así, por ejemplo, la utilización de computadoras en la industria, el comercio, la administración pública, en instituciones bancarias y financieras.

Esta verdadera invasión de la computadora en todos los ámbitos de las relaciones socioeconómicas ha motivado que muchos discurran ya de una auténtica "era informática". En efecto, pocas dimensiones de nuestra vida no se ven afectadas, dirigidas o controladas por el ordenador, ya sea de manera directa o indirecta; incluso, en determinados casos, las computadoras no sólo son utilizadas como medios de archivo y procesamiento de información, sino que, además, se les concede la capacidad de adoptar automáticamente decisiones. El problema surge cuanto a este

fenómeno se traduce en buscar fórmulas efectivas de control, respecto a las cuales el Derecho ha de tener un marcado protagonismo, en su papel de regulador de las relaciones y mecanismos sociales para el mantenimiento de un orden social. Nadie duda que el fenómeno informático produzca en distintas ramas del ordenamiento jurídico, llámese Derecho Civil, Procesal Civil, Mercantil, etcétera; un cierto trastorno al momento de enfrentar tales hechos, en un primer momento, las figuras delictivas tradicionales, en particular, los delitos patrimoniales, han tenido que hacer frente a esta nueva forma de criminalidad, pero, como veremos más adelante, éstas no ofrecen una delimitación típica completa frente a las nuevas conductas delictivas, razón por la cual en muchas legislaciones se tiende a crear tipos penales especiales referidos al delito informático.

Recordemos que el Derecho Penal, en los últimos treinta años, ha variado en gran medida sus formas y ámbitos de intervención, en algunos casos –con base en los principios de fragmentariedad, subsidiariedad y mínima intervención, según los cuales el *iuspuniendi* deberá ejercerse tan sólo ante las más graves vulneraciones de los intereses sociales más importantes y siempre que no existan formas de control social menos gravosas que el control penal - el derecho punitivo ha retrocedido en su espacio de acción, descriminalizando algunas conductas punibles y, en algunos otros, ha creído conveniente la represión de nuevas conductas consideradas socialmente dañosas, el cambio social operado en las últimas décadas, resulta íntimamente vinculado a la evolución tecnológica operada en este transcurso de tiempo, generándose problemas para la protección de intereses sociales no convencionales y para la represión de las conductas delictivas realizadas a través de medios no convencionales pues como bien precisa Zaffaroni: "El impacto de la explosión tecnológica es un problema que la política criminal conoce sobradamente. La técnica siempre es un arma y cada avance fue explotado criminalmente, en forma tal que siempre el criminal está más tecnificado que la prevención del crimen", lo que resulta más dramático en las sociedades informatizadas, en la medida que éstas resultan tecnológicamente vulnerables. Dentro de este fenómeno de nueva incriminación aparecen conductas que vulneran bienes jurídicos no convencionales y a su vez

comportamientos que se realizan empleando medios no convencionales para lesionar bienes jurídicos convencionales Ambos, por lo general, tienen intrínsecas connotaciones tecnológicas, debido a la incidencia que la evolución tecnológica, ha tenido en el cambio social, tal como hemos afirmado.

Los bienes jurídicos que tienen contenido relacionado a las nuevas tecnologías suelen ser reconocidos como tales, de manera primigenia, en los ordenamientos penales de aquellas sociedades de alto desarrollo industrial y comercial al ser los primeros en contar con necesidades de protección jurídico – penal, es así como en el ámbito internacional se produjeron diversas reacciones legislativas, las primeras surgieron, como detalla Cafure de Battistelli, "en los 70 referidas al ámbito de la intimidad; en los 80 y 84 lo referido al resguardo de la propiedad intelectual de los programas (software); en los 90 el desarrollo de nuevos paradigmas reguladores del derecho a la información".

Así, los países desarrollados orientaron sus esfuerzos dogmáticos y político – criminales, por un lado, a la lucha contra el delito cometido a través de medios informáticos y, por otro lado, a conferir protección jurídica a la información, atendiendo al nuevo significado que ella posee tal necesidad, generada desde comienzos de década en sociedades altamente informatizadas, se ha trasladado a sociedades como la nuestra, el reflejo de los avances tecnológicos ha tenido gran influjo en el campo de la criminalidad en tanto este nuevo *"modus operandi"* permite captar vacíos en el Derecho Penal tradicional, quedando indefensos "los contenidos inmateriales del sistema informático, su integridad, su disponibilidad o su exclusividad"; esta *"computerdependency"* (dependencia a la computadora), en la que – como puntualiza Gutiérrez Francés – "toda las sociedades modernas están involucradas", ha originado a su vez la posibilidad de utilizar las modernas tecnologías con fines delictivos, a continuación se detallará las causas que han generado que la informática se convierta en un fenómeno social trascendente incluso al ámbito criminal. Ahora, compartiendo el pensamiento de Luis Miguel Reyna Alfaro , se consideran cinco las causas coadyuvantes a que la informática constituya

un fenómeno social y adquiera importancia vital en el campo del Derecho Criminal**,** ya sea como objeto de protección o como medio actual e idóneo para la comisión de ilícitos penales; estas causan son:

el desarrollo tecnológico, la globalización de mercados y economías, la masificación de la informática, las debilidades propias de los sistemas de información y la dificultad probatoria, las mismas que a continuación analizaremos:

a) Desarrollo Tecnológico.- El avance en este aspecto permite el alcance cada vez más significativo de esta disciplina, un mayor desarrollo que se manifiesta en la modernidad de sus componentes, lo cual permite unidades de Hardware y Software más eficientes y veloces en el manejo de la información. Tan sólo basta con ver la enorme evolución operada en unos pocos años; de los ordenadores de dimensiones macroscópicas a los ordenadores portátiles que hoy en día operamos (*Personal Computers* o PC`S), ello nos permite apreciar la importancia del referido avance que estamos seguros no se detendrá, generando mayores perspectivas en esta disciplina.

b) Globalización de Mercados y Economías.- Causa que ha permitido el intercambio mercantil y económico fluido y constante entre naciones geográficamente lejanas y modelos económicos dispares, en virtud del aporte de elementos como las redes de interconexión que permiten que dicho intercambio comercial sea adecuado.

La Economía es, sin duda alguna, el bastón del actual modelo social, la existencia de bloques económicos en tenaz competencia en su afán de acaparar el mercado hacen que se requiera de elementos que favorezcan la obtención del lucro requerido, la Informática se convierte así en un elemento vital para sus aspiraciones. Asimismo, tal fenómeno de globalización permite el ingreso fluido y constante de material informático, tanto Hardware como Software, a los países de Latinoamérica, lo que genera la reducción de sus costos y en consecuencia posibilita su mayor empleo en

nuestras sociedades, lo que genera intrínsecas repercusiones en el campo del Derecho.

c) Masificación de la Informática.- Como respuesta a la situación concreta planteada con anterioridad como es la globalización de mercados y economías, que hace necesaria la aplicación de la informática para obtener eficientes resultados en materia financiera y teniendo en cuenta además que el avance tecnológico permite adquirir unidades de hardware y software a precios cada vez menores, encontramos que esta disciplina se viene convirtiendo más que en un lujo, un elemento accesorio, en una herramienta necesaria, en un elemento de trabajo; lo que implica su mayor utilización y por ende su masificación, como muestra de ello podemos apreciar que se ha convertido en un importante elemento logístico de ayuda al aparato jurisdiccional, función plasmada en las actuales reformas, tenemos así que tanto el Ministerio Público como el Poder Judicial han implementado casi en su totalidad el empleo de medios informáticos, así tenemos que el Ministerio Público desde el año 1992 ha instalado el Registro Único de Denuncias y Expedientes (RUDE), el mismo que fue sustituido posteriormente por el Sistema Integral de Apoyo a Labor Fiscal (SIAFT), lo cual con ello permite obtener información relativa al estado y evolución de las denuncias y procesos tramitados en dicha entidad; por otra parte, el Poder Judicial desde el año 1996 ha incorporado también en este tipo de recursos, desde las instancias primarias hasta la Corte Suprema de la República, ello ha significado un importante logro en lo que concierne a la celeridad que debe existir en el aparato jurisdiccional y uno de los más importantes aportes de la Reforma Judicial que se viene produciendo, es por ello que hoy en día nos es común ver un sinnúmero de establecimientos comerciales, de servicios, profesionales, estudiantes, etc., que hacen uso de la informática como elemento de producción, de trabajo, entre otros.

d) Las Debilidades Propias de los Sistemas de Información.- Las debilidades de la redes de información y en especial de La Internet se pueden simplificar en el hecho que sus mecanismos de operación permiten la introducción de terceros en sus

sistemas, así como la interceptación de los mensajes de los usuarios, esta indefensión, desde luego, provoca un sinnúmero de posibilidades en ámbito criminal. Es por este motivo que uno de los problemas de mayor análisis en el presente momento es la seguridad en las redes de información, de allí que la eficiencia y solidez de una empresa, entidad u organismo se mida actualmente en función a la seguridad que ofrecen sus sistemas de información.

e) Dificultad Probatoria.- El empleo de este medio acarrea un singular problema para el investigador, para el Juez penal, debido a la dificultad probatoria que su empleo para tales fines produce, es de observar con ello que la tecnificación de medios analizada no está aparejada con la capacitación necesaria en los órganos jurisdiccionales existiendo la posibilidad de que el delito cometido bajo tales circunstancias quede impune, a ello se aúna la falta de control efectivo que existe en estos sistemas de interconexión, situación de la que algunas personas abusan, ya sea creando páginas lesivas a determinados bienes jurídicos, interfiriendo en la información ajena, concertando voluntades o suprimiéndolas, es decir determinado su uso para fines delictivos, tal como más adelante será analizada.; no obstante, cabe aclarar que ninguna de las razones expuestas precedentemente pretende ser causa única e impostergable, considerando que la conjunción de las mismas produce el efecto materia de investigación, creando las condiciones necesarias para hacer de los medios informáticos un instrumento atractivo en el ámbito criminal. Por su parte, el derecho penal viene a colación debido a que es un Derecho de última ratio y medio de ejercicio del iuspuniendi del Estado, por lo que regula las sanciones para determinados hechos que constituyen violación de normas de Derecho y en este caso del Derecho Informático, en materia del delito Cibernético o Informático; es una fuente de conocimiento para hechos delictivos de características sui generis.

Igualmente, los Derechos Humanos, son indispensables para defender los derechos fundamentales del hombre, tales como la vida, la igualdad, la privacidad y la intimidad. El Derecho Informático y los medios que provee juegan un papel fundamental en el buen funcionamiento de los órganos jurisdiccionales, en la

eficiencia del manejo de las leyes y en la celeridad procesal, lo que garantiza procesos justos y resguardo de las garantías procesales. Además se relaciona con los derechos a la privacidad y la intimidad, frecuentemente vulnerados a través de medios informáticos como internet, redes sociales y otros usos que son únicamente atacables como delitos informáticos.

La propiedad intelectual interactúa con el Derecho Informático en sede de figuras como los plagios, la piratería y otros ilícitos que atentan contra los Derechos del Autor o de Propiedad Industrial, debido a que se utilizan los medios informáticos y sus vulnerabilidades para cometer estos actos.

siguiendo otra línea de pensamiento, debemos tratar la trama de la regulación jurídica del Derecho Informático. En la especialidad penal existen protecciones privativas y no privativas, aquellas que llevan implícito o no el derecho de última ratio, donde nos encontramos ante la posibilidad de ser sometidos a una sanción de privación de libertad. Dentro de las normas no privativas se encuentran: la protección penal que trata de aplicar normas sobre violación de secreto de empresas y corrupción administrativa ;y la protección civil en el marco contractual o extracontractual que incluye responsabilidad civil, concurrencia desleal y enriquecimiento sin causa. La privativa se da mediante un mecanismo sui géneris de protección, como lo es la propiedad intelectual ya sea por vía de Derecho de Autor o por la vía de Propiedad Industrial.

Actualmente, se emprenden procesos renovadores en el tema legislativo con ánimos de adecuar las normativas vigentes a las especificidades de la era informática y los nuevos desafíos como los contratos electrónicos, la firma digital, los open access, la sociedad del conocimiento, las contradicciones con el Derecho de Autor y la Propiedad Industrial, la información digital y las nuevas tecnologías, son fenómenos que a pesar de su reciente aparición merecen un tratamiento especial por parte del derecho.

2.13.- La criminalidad informática en la "sociedad de riesgos"

El conocido sociólogo Ulrich BECK ha puesto de manifiesto, que las sociedades modernas aparecen actualmente como verdaderas "sociedades del riesgo", en las cuales los efectos adversos del desarrollo de la tecnología, la producción y el consumo adquieren nuevas dimensiones y provocan riesgos masivos a los ciudadanos, los ejemplos más característicos los ubicamos en el tráfico vehicular, la comercialización de productos peligrosos o la contaminación ambiental.

En este contexto aparece la informática que si bien tiene innegables efectos positivos en el desarrollo social actual, tiene también un cariz negativo que puede identificarse con los "nuevos riesgos" que supone la actual configuración social; la criminalización de los delitos informáticos aparece así dentro del proceso de **"expansión del Derecho penal"**, caracterizado por la inflación de ésta rama del ordenamiento jurídico. Algunas distinciones teóricas entre los "delitos computacionales" y los "delitos informáticos"; hacer algunas precisiones conceptuales respecto a lo que constituye un delito "computacional" y lo que viene a ser un delito "informático" servirá no sólo para dilucidar uno de los aspectos que mayor confusión ha provocado en la doctrina penal, sino que será útil también para fijar los límites y pretensiones de la presente exposición.

a) El delito computacional.- viene a ser aquella conducta en que los medios informáticos, utilizados en su propia función, constituyen una nueva forma de atacar bienes jurídicos cuya protección ya ha sido reconocida por el Derecho penal, el ejemplo más característico lo ubicamos en el delito de Hurto cometido mediante "sistemas de transferencia electrónica de fondos, de la telemática en general o violación del empleo de claves secretas".

b) El delito informático.- propiamente dicho es aquel que afecta un nuevo interés social, un nuevo bien jurídico- penal que identificamos como: "la información (almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos)"; aunque para algunos autores como MAGLIONA MARKOVICTH/ LÓPEZ MEDEL, dicha distinción carece de trascendencia, las

consecuencias metodológicas que su utilización conlleva son, sin duda, importantes, en la medida que nos permite utilizarla como criterio diferenciador del bien jurídico y, ulteriormente, como opción de política criminal para el combate de la denominada "criminalidad mediante computadoras".

2.14.- Los delitos informáticos en el derecho penal

Es indudable que, así como las computadoras se presentan como herramientas muy favorables para la sociedad, también se pueden constituir en un instrumento u objeto en la comisión de verdaderos actos ilícitos. Este tipo de actitudes concebidas por el hombre (y no por la máquina) encuentran su génesis en el mismo surgimiento de la tecnología informática, ya que como es lógico pensar que de no existir las computadoras, estas acciones no existirían.

Por otra parte, la misma facilitación de labores que traen consigo dichos apartados propicia que, en un momento dado, el usuario se encuentre ante una situación de ocio, la cual canaliza a través de las computadoras, cometiendo sin darse cuenta una serie de ilícitos. Asimismo, por el propio egoísmo humano se establece una especie de duelo entre el hombre y la máquina, lo cual en última instancia provoca el surgimiento de ilícitos en su mayoría no intencionales, por ese deseo del hombre de demostrar su superioridad frente a las maquinas, y en este caso específico frente a las computadoras.

Esa facilitación de labores a que se ha hecho alusión, permite pues, que el estar redactando esas líneas, desde la tranquilidad de un hogar, se esté entrelazado por medio de la tecnología digital con información proveniente desde los puntos más lejanos del mundo, o tener el acceso a nuestras cuentas corrientes, o simplemente encontrarnos leyendo las noticias nacionales e internacionales, sin necesidad de recurrir al diario de papel o estar en contacto con nuestros familiares en todo momento, ubicación y situación posible. Todos estos alcances en la comunicación se han ido posicionando en nuestras vidas, lo que para nosotros es nuevo y novedoso, futuras generaciones recordaran estos tiempos como el comienzo de una nueva era, "la era digital y de la globalización de las comunicaciones".

El desarrollo de toda esta infraestructura en las comunicaciones, informaciones y negocios, que cada día más vemos compenetrados en las actividades políticas, culturales y comerciales de nuestro Perú, han mostrado un amplio crecimiento y desarrollo de todas las áreas del quehacer nacional, fenómeno mundial que ha ocasionado que el área dedicada a la informática y la computación ganen cada día más un espacio. Las tecnologías de la sociedad de la información pueden utilizarse, y se utilizan, para perpetrar y facilitar diversas actividades delictivas. En manos de personas que actúan de mala fe, con mala voluntad, o con negligencia grave, estas tecnologías pueden convertirse en instrumentos para actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público. Estas nuevas herramientas son usadas por personas, que por naturaleza humana nos hace enfrentar situaciones que se alejan de un claro comportamiento de convivencia en sociedad, en que con sus acciones utilizan para sí y en desmedro de otras nuevas técnicas de criminalidad para el cometido de sus acciones perturbadoras. Estas acciones perturbadoras de la convivencia social han nacido al amparo de las nuevas herramientas tecnológicas, ante lo cual en el ámbito mundial, se ha generado una percepción de la seguridad informática, percepción que se ha ido desarrollando muy por detrás de la realidad de los alcances de los llamados ciberdelitos, pero que ha generado acciones claras y evidentes de una necesidad de control por parte de los organismos de control social formal; es por ello que las experiencias desarrolladas por la Organización de las Naciones Unidas, la Comunidad Europea, los Estados Unidos de Norteamérica, se han dirigido hacia la creación de los organismos necesarios para plantear que el problema del cibercrimen y sus consecuencias en la seguridad de las personas y en sus respectivas economías es un hecho grave y que requiere de urgentes medidas de todo tipo, tanto en el ámbito legislativo, de tecnologías y de socialización.

Esta situación de vulnerabilidad a que nos vemos enfrentados día a día, no ha detenido el avance de otros medios, provenientes de las misma área tecnológica, para los resguardos de nuestros bienes jurídicos, tales como la privacidad, bienestar, derechos de autor, entre otros; como son la aparición en el ámbito privado de servicios que mediante el uso de nuevas tecnologías o metodologías permiten un

ambiente de tranquilidad relativa, especialmente en el desarrollo del comercio electrónico, es por ello, y luego de haber recorrido las líneas que anteceden, que antes de iniciar con el desarrollo de éste capítulo, es menester señalar que para poder determinar la posible existencia de los delitos informáticos, es necesario determinar que se debe recurrir precisamente a las dos materias que integran la relación de la que se ha estado hablando y sosteniendo en todo el decurso de la presente disquisición, como son la informática y el derecho, en la cual cada una aporta su horizonte y terreno de proyección.

Si nos remitimos a la dogmática penal, específicamente a la Teoría del Delito, ésta nos dice que el delito es la conducta típica, antijurídica y culpable a la que se asocia una pena como consecuencia. Afirmada la existencia del delito, procede la consecuencia o aplicación de la pena, sabemos que, entre una gran cantidad de conductas posibles, sólo algunas son prohibidas por el legislador. Para poder distinguir las conductas que son delitos de aquéllas que no lo son, acudimos a los dispositivos legales que describen las conductas prohibidas; por ello, no habrá delito, pues, cuando la conducta de un hombre que utiliza las computadoras y/o su tecnología no se adecua a alguno de esos tipos penales; por otro lado, cuando necesitamos averiguar qué es delito informático, necesariamente se debe de buscar la respuesta en la parte especial del Código Penal, específicamente en lo atinente a los delitos informáticos. De lo señalado, nos impele además, en consultar la doctrina nacional y extranjera para conocer las diversas conductas a las que se les da el nombre de delitos informáticos y, posteriormente, examinar si se adecuan o no a los tipos previstos en las leyes penales vigentes, los aportes de los criminólogos han sido muchos, gracias a ellos se detectaron graves situaciones como el olvido a las víctimas, los crímenes de los poderosos o pudientes, los aplausos de poder, se enfatizó el papel selectivo del sistema penal como filtro de situaciones vulnerables, etcétera (como se atisba, es difícil que no recurran a términos jurídico-penales como lo es crimen o delito).

La desventaja, creemos, se puede encontrar en la confusión de llamar por un lado "delito" o "crimen" a lo que posiblemente sólo sea una conducta indebida, ilícita o ilegal, y que en el campo de la informática podrá ser considerada digna de protección penal en el futuro; bajo esta perspectiva, debemos de considerar que para los criminalistas la noción de crimen, delito, ilícito, podría connotar situaciones diferenciadas y conceptos disímiles; y cuando no necesariamente reguladas por la legislación nacional.

Con lo referenciado procedentemente, podemos adelantar una apreciación respecto a lo que se considera el delito informático o llamado por algunos como delito por computadora, como cualquier acto ilícito penal en el que las computadoras u ordenadores, su técnica y funciones desempeñan un papel ya sea como método, medio o fin. Por otro lado la doctrina dominante sobre estos aspectos, vierte ciertas definiciones al respecto, entre las cuales tenemos las que definen al delito informático como aquella conducta ilícita en que se utiliza una computadora como instrumento u ocupación criminal; como aquella acción ilegal en el que la computadora es instrumentando u objeto de delito y asimismo que los delitos informáticos son cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o transmisión de datos. Como se observa, son múltiples las definiciones que sobre los delitos informáticos la doctrina se ha encargado de elaborar, pero por ahora es menester abocarnos a tratar a continuación el aspecto vinculante entre el fenómeno informático y el derecho penal.

2.15.- Concepto de delito informático:

Antes de adentrarnos al tratamiento de tema, es menester delimitar conceptualmente lo que entenderemos por delito, trayendo para ello a colación la opinión del maestro carrara, para quien delito es aquella *infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, resultantes de un acto externo del hombre, positivo o negativo, moralmente imputable y políticamente dañoso*.

Para Beling, el delito es una acción típica antijurídica, culpable, subsumible bajo una sanción penal adecuada y que satisfaga las condiciones de punibilidad. En el año 1930 modifica sustancialmente su definición señalando: que *el delito es acción típicamente antijurídica y correspondientemente culpable, siempre que no se dé una causa legal de justificación.*

Para el maestro Luis Jiménez de Asúa, lo conceptúa como un acto típicamente antijurídico imputable al culpable, sometido a veces a condiciones objetivas de penalidad, y que se halla conminado con una pena o, en ciertos casos, con determinada medida de seguridad en reemplazo de ella; por otro lado, para el profesor colombiano, Juan Fernández Carrasquilla, define al delito como un injusto culpable, un acto antijurídico realizado típicamente dentro de los límites de la responsabilidad subjetiva; y añade el autor que, lo determinante son los paradigmas o las descripción en la ley de los modelos abstractos o figuras delictivas mediante la técnica de la tipificación en un sentido jurídico, podemos definir el delito como acción típicamente antijurídica y culpable; resulta de las definiciones anteriores, que para que un acto sea delito son necesarios estos requisitos:

a) El delito es un acto humano, es una acción (acción u omisión).

b) Dicho acto humano ha de ser antijurídico, ha de estar en oposición con una norma jurídica, debe lesionar o poner en peligro un interés jurídicamente protegido.

c) Debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.

d) El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

e) La ejecución u omisión del acto debe de estar sancionada por una pena.

En otra línea de pensamiento, los conceptos de fraude y delito son disímiles, y es menester en esta estación acrisolar, señalando que el **fraude,** puede ser definido como el engaño, la acción contraria a la verdad o a la rectitud. La definición de delito es más compleja, como lo hemos advertido líneas atrás, y han sido pues muchos los intentos de formular una noción de delito que sirviese para todos los tiempos y en todos los países. Y es que esto no ha sido posible, dada la íntima conexión que existe entre la vida social y jurídica de cada sociedad y cada siglo, ya que ambas se condicionan íntimamente, recordemos que artículo 11 del Código Penal de 1991, preconiza que ***son delitos y faltas las acciones u omisiones dolosas o culposas penadas por la ley*.** De lo que se advertiría que ésta es una noción meramente formal, y que no define cuáles son sus elementos integrantes, que como vemos, ya se detalló anteriormente.

Con las nociones referenciadas, podemos ensayar una aproximación al concepto de delito informático, señalando que son aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático**;** de ello se tiene que el delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, estafas, etcétera; sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

En la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir un concepto propio de los llamados delitos informáticos, aún cuando no existe dicha definición con carácter universal, se han formulado conceptos funcionales atendiendo a las realidades concretas de cada país: **"delito informático es toda aquella conducta ilícita que hace uso indebido de cualquier medio informático, susceptible de ser sancionado por el derecho penal".**

También se entiende al delito informático como "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena o como mero símbolo"; "Como aquel que se da con la ayuda de la informática o de técnicas anexas".

Por ello, muchas discusiones se han planteado entorno al concepto del delito informático-computer crime o computer kriminalitat ; para algunos autores éste no es más que el **delito cometido bajo el empleo de medios informáticos,** es decir, constituyen nuevas formas de comisión de conductas ya descritas en sede penal, rechazando la existencia de un bien jurídico autónomo para esta clase de delitos. Para otro sector de la doctrina el delito informático tiene un contenido propio, afectando así un nuevo interés social cuyo reconocimiento legislativo urge, diferenciando así entre delitos computacionales-como nuevas formas comisivas de delitos, y delitos informáticos, aquellos que afectan el novísimo del bien jurídico penal propuesto. Finalmente, existe una tercera vertiente, defendida por la doctrina de habla inglesa, que hace una diferencia tripartita en que la informática aparece como medio para cometer delitos tradicionales, como fin en sí misma y como medio de prueba.

Dentro del primer secyor se puede citar, en la doctrina extranjera, a Guibourg, Alende, Campanella, Parker y Viega Rodriguez, mientras que en la doctrina nacional a Bramont- Arias Torres, Núñez Ponce e, implícitamente, Biossiers Manzini, Calderón García y García Cantizano.

Según Guibourg, Alende, Campanella; "El llamado delito informático no constituye una nueva categorías delictiva. Los hechos ilícitos que se cometen (o se facilitan) mediante el empleo del ordenador son, en principio, los mismos que desde hace milenios las sociedades han castigado de una forma o de otra".

Parker señala que el delito informático es: " cualquier acto criminoso relacionado con la tecnología informática, por el cual una víctima ha sufrido una pérdida y un autor ha obtenido internacionalmente una ganancia", este autor, al hacer referencia a

aspecto estrictamente patrimonial (una ganancia y una pérdida), entiende que el bien jurídico lesionado con el delito informático que en **Patrimonio.**

A entender de María José Viega Rodríguez: "Los llamados delitos informáticos no constituyen una nueva categoría delictiva, sino que son los mismos delitos que ya se vienen castigando: delitos contra las personas, contra el honor, la libertad, la seguridad pública por la nación".

En la doctrina nacional, ha sido Bramont -Arias Torres el único penalista que ha analizado con cierto detenimiento el tema en estudio, el referido autor indica: " en realidad no existe un bien jurídico protegido en el delito informático, porque en verdad no hay como tal un delito informático. Este no es más que una forma o método de ejecución de conductas delictivas que afectan a bienes jurídicos que ya gozan de una específica protección por el Derecho Penal, afiliándose así la postura antes referida.

Núñez Ponce, especialista en Derecho Informático, se afilia también a esta postura al precisar: " En el plano de la Dogmática Jurídico-Penal, la criminalidad informática puede suponer una nueva versión de delitos tradicional".

La postura de Blossiers Manzini y Calderón García resulta bastante singular, expresar: " Parece ser que lo que en realidad vulnera ésta novedosa tipología es una violación mixta de valores jurídicos, que en algunos casos compromete tanto al patrimonio como a la libertad de las personas o el sistema informático y la protección de datos", es decir, identifican los intereses afectados, con el delito informático con valores que ya gozan de determinada tutela penal (patrimonio, intimidad, etcétera), con el añadido de la pluriofensividad de la conducta, así las cosas, no identifican realmente un nuevo bien jurídico, sino que se limitan a subrayar un probable concurso de delitos. Sin embargo, entran en contradicciones al afirmar más adelante; "esta clase de ilícitos atentan contra la intimidad de las personas e inclusive puede

darse el caso de que la misma vea violada su intimidad, sino que su identidad pueda ser sustituida".

La profesora García Cantizano ha ingresado al debate, considerando que si bien en el Derecho Penal no existe un concepto unánime sobre lo que es la delincuencia informática, considera que el delito informático puede definirse, en términos generales, como: "aquel en el que para su comisión se emplea un sistema automático de procesamiento de datos o de transmisión de datos", con lo que excluye la existencia de un nuevo interés social.

Un segundo sector diferencia entre ambas situaciones, esto es, en primer lugar, el uso de la informática como medio novedoso para afectar bienes jurídicos ya resguardados en clave penal, lo que se ha dado por llamar "delito computacional", en tanto que en segundo lugar cataloga aquellas conductas que afectan un nuevo interés social.

El delito computacional es aquella conducta que empleando tecnología de la información vulnera bienes jurídicos reconocidos penalmente- por ejemplo, las ofensas a través de redes de interconexión como el internet afectan el bien jurídico tradicionalmente conocido como honor, constituyendo incluso modalidad agravada del delito de Difamación - sin embargo, debe subrayarse que dentro de este rubro sólo debe comprenderse a las conductas que utilicen los componentes informáticos (software y hardware) en su propia función, por lo cual no cabria considerar como delito computacional, por ejemplo, las lesiones causadas empleando como objeto contundente un monitor de computadora, pues, como resulta evidente, el elemento material denominado Hardware no ha sido empleado en la función que tiene asignada.

Por otra parte, aparece el delito informático en sentido estricto y que sería más bien aquella conducta que afecta un nuevo interés social, íntimamente ligado al tratamiento de la información; en principio, resulta evidente que existe diferencia

entre ambos conceptos (delito computacional e informático), sin embargo lo cierto es que ambos forman parte de un mismo fenómeno criminal, que deberá denominarse "criminalidad mediante computadoras" ; en este sentido se han pronunciado autores como Pérez Luño, Jijena Leiva, Lima, Tellez Valdez, Davara Rodríguez, Baon Ramirez, Herrera Bravo/Zavale/Berltramone, Gutiérrez Francés González Rus, Adamski y Tiedemann, entre otros.

Es el concepto de Pérez Luño donde se observa con mayor claridad esa diferenciación al indicar que la criminalidad mediante computadoras comprende " aquel conjunto de conductas criminales que se realizan a través de un ordenador electrónico, o que afectan el funcionamiento de los sistemas informáticos; para Jijena Leiva la " criminalidad mediante computadoras" se puede definir como: toda acción típica, antijurídica y culpable, para cuya consumación se usan la tecnología computacional o se afecta a la información contenida en los sistemas de tratamiento automatizado de la misma (delito informático propiamente tal), aunque incurra-según creo-en el error de comprender a las conductas aún no tipificadas como delitos en el ordenamiento penal.

María de la Luz Lima, define el crimen mediante computadoras como " cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñen un papel ya sea como método, medio o fin". Otras definiciones citadas por dicha autora, tenemos la de considerar a los delitos informáticos como aquellos en que se utiliza a una computadora como instrumento u ocupación criminal o como cualquier acción ilegal en el que la computadora es el instrumento u del delito, algunos autores prefieren hablar de abuso de computadoras señalando que son aquéllos asociados con la tecnología de la computadora en el cual una víctima ha sufrido una pérdida y del autor intencionalmente ha obtenido una ganancia.

Regresando a la primera definición anotada sobre delito por computadora, Lima menciona ejemplos de delitos clasificados según el papel de la computadora, y así nos habla: como método, y cataloga el fraude, robo, robo de servicios no autorizados; como medio: se refiere al acceso no autorizado para extorsionar, la información, y

como fin: al señalar la destrucción de programas, daños a la memoria, entre otros, como se puede determinar, de las anteriores definiciones no se desprende un delito o con naturaleza propia, sino que puede ser cualquiera cometido por medio de la computadora o teniendo a esta por objeto; por su parte, Julián Téllez Valdéz, en una línea bastante cercana a la de la Profesora María de la Cruz Lima, emite una definición bastante elemental y acertada a su vez, en la medida que considera el delito informático a aquellas conductas, típicas o no, en las que se tienen a la computadora como instrumento o fin; acotando de manera sensata, el Profesor Ramiro Salinas Siccha, nos alcanza una definición acerca del delito informático, señalando que son aquellas conductas típicas, anti jurídicas culpables y punibles, en las que la computadora, sus técnicas y funciones desempeñan un papel trascendente, ya sea como método, medio o fin en el logro de los objetivos indebidos del agente, cuál es el logro de algún perjuicio de tipo patrimonial a su víctima. Agrega el citado autor, que también se le podría definir a los delitos informáticos como aquella conducta típica, antijurídica, culpable y punible en la que la gente hace uso de cualquier medio informático para obtener un beneficio indebido en perjuicio del sujeto pasivo.

Davara Rodríguez y Baon Ramires, parten de similar línea de argumentación, pues califican como delito informático aquellas acciones que reuniendo las características del delito, sean realizadas empleando un método informático o vulnerando los derechos del titular de un elemento informático, sin embargo, el primero de los nombrados considera que si bien dicha categoría del delito, lege lata, no existe, admite la conveniencia de su utilización.

Herrera Bravo, Zavale y Beltramone, definen el delito informático como: toda conducta que revista características delictivas, es decir, sea típica, antijurídica o culpable, y atente contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del empleo de las tecnologías de la información y el cual se distingue de los delitos de las computadoras o tradicionales informatizados, sin embargo, al igual que Jijena Leyva,

excluyen las conductas aún no tipificadas, lo que a criterio y parecer de la doctrina dominante, no sería lo más conveniente.

2.16.- El bien jurídico en el delito informático:

A. Nociones Generales.

Los constantes avances tecnológicos en materia informática han propiciado la aparición de nuevos conceptos, generando asimismo la modificación de otros tantos, enriqueciéndolos en la mayoría de ocasiones, así el contenido del término **"información"**, que según la definición de la Real Academia de la Lengua Española significa: "enterar, dar noticia de algo" y que en términos legos hubiera significado tan sólo una simple acumulación de datos, se ha ampliado, transformándose como advierte Gutiérrez Francés: «en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico» y es que, como recientemente ha puesto de manifiesto Vargas Gómez-Urrutia: "En ésta sociedad, la información y los servicios que la misma ofrece han pasado a ser una *resintracommercium*; esto es, un bien de consumo cuyo valor económico es muy elevado".

Hoy en día no resulta suficiente poseer la información, es necesario además tener la capacidad de almacenarla, tratarla y transmitirla eficientemente, de allí que "la información" deba ser entendida como un proceso en el cual se englobe los tres supuestos (almacenamiento, tratamiento y transmisión), el almacenamiento, tratamiento y transmisión de datos mediante los sistemas de procesamiento e interconexión conceden el novísimo significado atribuido al término información , colocando a su poseedor en una privilegiada situación de ventaja respecto al resto de individuos, pues nadie puede dudar que quien ostenta la información y sepa almacenarla, tratarla transmitirla correctamente mediante los sistemas procesamiento de datos, será quien obtenga mayores dividendos en sus actividades económicas, fin primordial perseguido en este tipo de actividades, por lo que debe ser considerado un

Valor económico de empresa, aunque debe entenderse que al adoptar el vocablo " empresa" nos referimos a ella como actividad (industrial, mercantil, comercial), pues la protección que se pretende fundamentar no está dirigida a la empresa como sociedad (anónima, encomandita, individual, etcétera), sino que se orienta a la información y su nuevo significado en la actividad empresarial.

De allí que el denominado " nuevo paradigma económico", resulte ser un fenómeno comparable tan sólo con el ocurrido con la aparición de la electricidad, aunque en este caso el fenómeno haya resultado mucho más acelerado, por ello es que Alan Greenspan, Presidente de la Reserva Federal de los Estados Unidos, reconozca que la prosperidad económica de los últimos ocho años en dicho país y sus corporaciones resulta atribuible a la influencia de la informática; así podemos sostener que el interés social digno de tutela penal sería: «**la información** (almacenada, tratada y transmitida a través de sistemas informáticos), como valor económico de la actividad de empresa", ahora bien, habrá que determinar si estamos ante un bien jurídico penal individual o si más bien el interés tutelado es de carácter colectivo. Si tenemos en consideración que estamos ante un interés social vinculado a la actividad empresarial, toda vez que la información se convierte en un valioso instrumento de la actividad de empresa, **el bien jurídico "información"** se encontraría encardinado dentro de los llamados delitos socio-económicos y por ello sus repercusiones trascenderían a las propias bases del sistema socio- económico, esto es, estamos a través de bien jurídico colectivo; sin embargo, ello no obsta a que puedan resultar implicados, en determinados supuestos, intereses patrimoniales individuales, con lo cual surge el inconveniente adicional de **diferenciar entre los delitos patrimoniales y los referidos al orden socio-económico**, para ello debemos dejar en claro que el bien jurídico propuesto está dirigido a resguardar intereses colectivos, cercanamente relacionados al orden público económico, aunque puedan concurrir a su vez intereses individuales, que en éste específico caso serían los de los titulares de la información contenida en los sistemas de tratamiento automatizado de datos.

B. Consideración de la "información" como bien jurídico penal.

Es proficuo en sostener, que en cada nueva incriminación penal surge una aparente contradicción con los principios de exclusiva protección de bienes jurídicos del derecho penal, entendido como última ratio, sin embargo, es imprescindible señalar que el principio de intervención mínima, se sustenta en un conjunto de procesos de entrada y de salida, de criminalización y des-incriminación, resultando de la normal y obligada evolución social que genera la sustitución de bienes jurídicos, los nuevos intereses sociales suplen a los bienes jurídicos que por variación temporal de las necesidades político criminales se han convertido en poco dignos de tutela penal.

El principio de exclusiva protección de bienes jurídicos se encuentra previsto, de manera implícita, en el art. IV del título preliminar del código penal peruano que señala: " *la pena necesariamente precisa de la elesión puesta en peligro de bienes jurídicos tutelados por la ley"*. Sin embargo, pese a la postura del legislador peruano, las recientes reformas en el ámbito penal llevan a reflexionar sobre la verdadera aplicación de dicho principio, la presencia de un interés social vital no acredita a la existencia de un bien jurídico penalmente relevante, es necesario también que éste reúna los requisitos de merecimiento o importancia social y necesidad de protección en sede penal, principios de una concepción del bien jurídico penal de índole político criminal.

Respecto a la valoración del merecimiento de protección o importancia social del interés debe tenerse en claro que éste se refiere como dice Rodríguez Mourullo, a la generalidad de los componentes del equipo social y no sólo a la minoría o un sector social determinado, no obstante, la valoración de aquellos intereses que, como la información, tienen un inmanente carácter colectivo, debe observarse en función a su trascendencia para los individuos, lo que se correspondería a los lineamientos propios del modelo de Estado Social y Democrático de Derecho, de esta manera, como señala Mir Puig, " la valoración de la importancia de un determinado interés

colectivo exigirá la comprobación del daño que cause a cada individuo su vulneración", es decir, no resulta suficiente para la comprobación del merecimiento de protección que el interés social trascienda a la generalidad, es preciso que su lesión o puesta en peligro posean entidad para provocar daño en los individuos integrantes del grupo social.

Si la cuestión se hubiese planteado algunos años atrás hubiese resultado, por decir lo menos, cuestionable afirmar la existencia de merecimiento de protección penal en el interés social " información", sin embargo, la situación resulta hoy en día menos complicada, el fenómeno informático en el que todas nuestras sociedades se hallaninmersas ubica al interés vital aquí planteado en una posición de absoluto y comprensible merecimiento de resguardo en sede penal, superándose de este modo el primer obstáculo.

Debe dejarse constancia sin embargo que ésta valoración no debe ser efectuada desde una óptica cuantitativa, lo que traería consigo negar la presencia de merecimiento de protección atendiendo a las estadísticas existentes sobre la materia, en las cuales se observa, verbigracia, que el 75% de los peruanos nunca ha usado una computadora, que tan sólo el 5 % de los internautas se encuentran en Latinoamérica (E.E.U.U. 57%, Asia 20%, Europa 16%, África y Medio Oriente 1% cada uno), que tan sólo el 7% de personas en nuestro país posee un ordenador en su casa (E.E.U.U. 65%, América Latina 16%) o que, sobre una base de 55 países, el Perú ocupe el lugar 49, según la *Information Society Index* (Índice de la sociedad de información).

La cuestión debe ser abordada atendiendo a la importancia cualitativa del interés propuesto, dado que todos los campos de la vida social han sucumbido al fenómeno informático, sin duda, responder a la cuestión de si el interés social " información" se encuentra necesitada de protección penal es un extremo delicado, a pesar de ello en el presente acápite se pretenderá acrisolar tales cuestiones.

La necesidad de tutela penal habrá de calificarse en atención a la eficacia de los demás medios de control social, en efecto, un interés social requerida de protección en sede penal cuando los demás medios con los que disponen las otras ramas del Derecho hayan fracasado pues, como bien subraya Berdugo, el Derecho Penal es sólo uno de los tantos instrumentos del control social existentes y posiblemente no sea el más importante de ellos, se puede decir que **la informática y la información**, como Valor económico, no tienen regulación específica en nuestro país, a diferencia de lo que ocurre en el derecho comparado, no obstante, existen normas que de alguna u otra forma hace referencia a ellas, así por ejemplo, la ley de Derechos de Autor; dedica dos capítulos específicos a la protección de los programas de ordenador (Título VI-disposiciones especiales para ciertas obras, Capítulo II-de los programas de ordenador, artículos 69 a 77) y de las bases de datos (Título VI -disposiciones especiales para ciertas obras, capítuloIII-de las bases de datos), en este caso, la protección jurídica se centra en los derechos intelectuales inmanentes a la creación de estos, la información encuentra resguardo en el ámbito del Derecho Industrial siempre que esté referida a un secreto de carácter industrial, por lo que la restricción en el radio de acción de la Ley de Propiedad Industrial; la hace insuficiente para afirmar la existencia de protección puntual de la información.

Otra vía a la cual se ha pretendido recurrir ha sido al proceso constitucional del habeas data, previsto tanto en nuestra Carta Política de 1993 y Código Procesal Constitucional, y que procede contra cualquier autoridad, funcionario o persona que vulnere o amenace los derechos contenidos en el artículo 02 incisos 05 y 06 de la Carta Magna; sin embargo, como precisa García Belaúnde, dicha acción ha sido parcamente utilizada, limitándose a la obtención de información que se guarda en la administración pública y que ésta no desea entregar; sin embargo, tampoco se puede sostener que por ésta vía pueda afirmarse la existencia de tutela especifica de la información como Valor económico, la protección que el "habeas data" brinda está dirigida a la "libertad informática", que pretende mantener a salvo a los ciudadanos, utilizando términos de Pérez-Luño, de "la omnipresente vigilancia informática de nuestra existencia habitual", en ésta línea de argumentación, la ausencia de

protección extra penal no evidencia, por sí misma, la carencia de necesidad de protección penal, empero, debemos tener en cuenta que existe necesidad de protección punitiva cuando "en el caso concreto no existe ningún otro medio disponible que sea eficaz y menos aflictivo"; el fracaso de los medios de control social y la dañosidad social propia de este tipo de conductas hace necesaria la regulación punitiva de comportamientos que afecten el bien jurídico aquí propuesto, al menos esa es la tendencia que se observa en la legislación comparada, de esta manera nos alejamos del sector doctrinal que considera que detrás del delito informático no existe un bien jurídico específico, tratándose tan sólo de formas de ejecución de delitos que afectan bienes jurídicos de protección penal ampliamente reconocida. Quienes sostienen esto confunden los delitos informáticos con los delitos computacionales, estos últimos se tratarían - como precisa Herrera Bravo " sólo de ilícitos convencionales que ya están regulados en el Código Penal", dejando en claro que los delitos informáticos son conductas nuevas que por su singular naturaleza no se subsumen en la descripción típica de los delitos convencionales.

C. De las conductas lesivas al bien jurídico penal

Debemos de partir en este apartado, señalando que ciertos comportamientos realizados a través de medios informáticos afectan bienes jurídicos tradicionales como el **hurto, la Estafa o las Falsedades Documentales**, sin embargo, al admitir la existencia de un bien jurídico propio y proviniendo éstas lesiones a bienes jurídicos de distinta índole, como el Patrimonio o la Fe Pública, no corresponde en éste tópico hacer referencia a la utilización de medios informáticos para la comisión de delitos convencionales, sino tan sólo a aquellos que lesionen o pongan en peligro el bien jurídico "información".

Las conductas lesivas a la información son, según el Consejo de Europa y el XV Congreso Internacional de Derecho, entre otras:

1. Fraude en el campo de la informática.
2. Falsificación en materia informática.
3. Sabotaje informático y daños a datos computarizados o programas informáticos.
4. Acceso no autorizado.
5. Intercepción sin autorización.
6. Reproducción no autorizada de un programa informático protegido.
7. Espionaje informático.
8. Uso no autorizado de una computadora.
9. Tráfico de claves informáticas obtenidas por medio ilícito.
10. Distribución de virus o programas delictivos.

2.17.- Los sujetos del delito informático

A.- Sujeto activo:

Las personas que cometen los "delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos, con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De ésta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente es tema de controversia ya que para algunos en el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas,

decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos; sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminológico norteamericano Edwin Sutherland en el año de 1943, efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aun cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios entre otros".

Asimismo, este criminológico estadounidense dice que tanto la definición de los "delitos informáticos" como las de los " delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto estatus socioeconómico, su comisión no puede explicárselo por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional, hay dificultades para elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; hay dificultades para descubrirlo y sancionarlo, en razón del poder económico de quienes los cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera así mismos "respetables" otra coincidencia que tiene estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo sino privativos de la libertad; por nuestra parte, consideramos que a pesar de que los "delitos informáticos" no poseen todas las características de los

"delitos de cuello blanco", sí coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo, que dada la naturaleza de nuestro objeto de estudio nos vemos en la necesidad de limitar.

B.- Sujeto pasivo:

En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del *modus operandi* de los sujetos activos.

Dado lo anteriormente mencionado, ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra"; asimismo, podríamos admitir que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección

eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento; en el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja a los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender de investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más; además, debemos destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

CAPITULO III

LEGISLACIÓN NACIONAL

3.1.- Ley de delitos informáticos en el Perú

En el Perú, por **Ley 30096**, se ha aprobado la Ley de Delitos Informáticos publicada el martes 22 de Octubre de 2013. Esta ley regula el ámbito jurídico informático penal y por su importancia consideramos necesario hacer una breve reseña.

3.2.- 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:

3.3.- Ley de delitos informáticos 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, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

3.4.- Delitos contra datos y sistemas informáticos.

Artículo 2. Acceso ilícito.- el que accede sin autorización a todo o 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 contra la integridad de datos informáticos.- el que, a través de las tecnologías de la información o de la comunicación, 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. El Peruano Martes 22 de octubre de 2013 **505485**

Artículo 4. Atentado contra la integridad de sistemas informáticos.- el que, a través de las tecnologías de la información o de la comunicación, 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.- 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.

3.6.- 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 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.

3.7.- 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.

3.8.- 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.

3.9.- 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 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 fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

3.10.- 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 El Peruano Martes 22 de octubre de 2013 **505486** 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.

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:

3.11.- Otros delitos, modificaciones y normas complementarias

La ley en comentario regula también delitos contra indemnidad y libertad sexuales. Asimismo, modifica en el Código Penal los delitos de interferencia telefónica, pornografía infantil y discriminación dándole coherencia y sistematización en relación a los delitos informáticos; por otra parte, modifica artículos del Código Procesal Penal y de la Ley contra el crimen organizado. Finalmente, cabe destacar que se dispone que: "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.

El Presidente del consejo de ministros del Perú, Juan Jiménez Mayor, en conferencia de prensa del 23 de octubre afirma; " La Ley De Delitos Informáticos". Protege el derecho a la intimidad y a la información personal de los ciudadanos, y de ninguna manera vulnera los principios de la libertad de expresión y prensa. La norma coloca Perú en el estándar internacional de lo que significa la protección de datos y de nuestra intimidad". Hay distintas posiciones sobre esta ley, lo esencial consideramos en su difusión, su análisis fundamentando y aplicación acorde con el ordenamiento jurídico y el derecho informático.

3.12.- Resumen de leyes y modificatorias en los últimos años 2013 –2014

Aprueban Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales viernes 22 de marzo de 2013 DECRETO SUPREMO Nº 003-2013-JUS EL PRESIDENTE DE LA REPÚBLICA La aprobación de la Ley N° 30076 en el Perú, 19 de agosto del 2013.

Modifica el Código Penal, Código Procesal Penal, Código de Ejecución Penal y el Código de los Niños y Adolescentes y crea Registros y Protocolos con la finalidad de Combatir la inseguridad ciudadana, según el título del Diario Oficial “El Peruano”.

Entre las modificaciones al Código Penal peruano, se destaca, el artículo 207-D, Mediante el cual se tipifica el tráfico ilegal de datos: *Artículo 207-D. Tráfico ilegal de datos.* Ley de Delitos Informáticos N 30096 publicada el martes 22 de Octubre de 2013 Esta ley regula el ámbito jurídico informático penal. LEY Nº 30171 LEY QUE MODIFICA LA LEY 30096, LEY DE DELITOS INFORMÁTICOS. 09 del mes de Marzo del año 2014.El cual Modifica los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos. El congreso de la república; ha dado la ley siguiente: adicionence los articulos 183-b y 183-c al codigo penal, en materia de pornografia infantil en internet

ARTICULO 1°. - Adicionase los artículos 183-B y 183-C al Capítulo XI -Ofensas al Pudor Público- del Código Penal, con el siguiente texto:

"Artículo 183-B. - Al que procure o facilite por cualquier medio el que uno o más menores de dieciocho años, con o sin su consentimiento, lo o los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos, o pornográficos con el objeto y fin de video grabarlos, fotografiarlos o exhibirlos mediante medios impresos, electrónicos o de un sistema de datos a través de cómputo o de cualquier otro mecanismo de archivos de datos, con o sin el fin de obtener un lucro, se le impondrán la pena privativa de libertad no menor de cinco ni mayor de doce años y con trescientos sesenticinco días multa".

"Al que fije, grabe, imprima actos de exhibicionismo corporal, lascivos o pornográficos, en que participen uno o más menores de dieciocho años, se le impondrá la pena de cinco a doce años de pena privativa de la libertad y de trescientos sesenticinco días multa. La misma pena se impondrá a quien con fines de lucro o sin él, elabore, produzca, reproduzca, ofrezca, venda, arriende, exponga, publicite, haga accesible, distribuya o trasmita a través de un sistema de computo o cualquier otro mecanismo de archivo de datos, el material a que se refiere el presente artículo".

"Artículo 183-C. - Para los efectos de estos artículos se entiende por pornografía infantil, toda representación de un menor de edad dedicado a actividades explícitas reales o simuladas de carácter sexual, realizada a través de escritos, objetos, medios audiovisuales, electrónicos, sistemas de cómputo o cualquier medio que pueda utilizarse para la comunicación y que tienda a excitar sexualmente a terceros, cuando esta representación no tenga valor artístico, literario, científico o pedagógico."

Artículo 2°. - La presente ley entrará en vigencia al día siguiente de su publicación en el Diario Oficial "El Peruano" - Lima, 09 de mayo de 2002 Enith Chuquival Saavedra Congreso de la República.

Res. N° 385-2013-CG.- Aprueban listado de entidades públicas que serán incorporadas al Sistema Electrónico de Registro de Declaraciones Juradas de Ingresos y de Bienes y Rentas en Línea en el año 2013**505500Res. N° 386-2013-CG.-** Aprueban Directiva "Disposiciones sobre el Procesamiento y Evaluación de las Declaraciones Juradas de Ingresos y de Bienes y Rentas de autoridades, funcionarios y servidores públicos; así como información sobre Contratos o Nombramientos, remitidos a la Contraloría General" y Directiva "Disposiciones para el uso del Sistema de Registro de Declaraciones Juradas de Ingresos y de Bienes y Rentas en Línea"**505501**

3.13.- Instituciones educativas.

Res. N° 1385-R-UNICA-2013.- Autorizan viaje de autoridades de la Universidad Nacional "San Luis Gonzaga" de Ica a Brasil, con la finalidad de firmar convenios específicos **505502**

3.14.- Jurado nacional de elecciones.

Res. N° 773-2013-JNE.- Declaran nula Resolución N° 064-2013-ROP/JNE emitida por el Registro de Organizaciones Políticas del JNE, nulo oficio de la Secretaría General de la ONPE y nulidad de todo lo actuado en procedimiento de inscripción solicitado por organización política **505503 Res. N° 899-2013-JNE.-** Declaran nulo Acuerdo de Concejo que declaró infundado pedido de vacancia presentado contra alcalde de la Municipalidad Provincial de Huamalíes, y disponen devolver los actuados para que se emita nuevo pronunciamiento **505508 Res. N° 933-2013-JNE.-** Convocan a ciudadana para que asuma cargo de regidora del Concejo Municipal de la Municipalidad Distrital de Ancón, provincia y departamento de Lima **505512 Res. N° 945-2013-JNE.-** Declaran nulo lo actuado en procedimiento de suspensión seguido contra alcalde de la Municipalidad Distrital de Ciudad Nueva, provincia y departamento de Tacna **505512 Res. N° 949-A-2013-JNE.-**Convocan a ciudadana para que asuma cargo de regidora de la Municipalidad Distrital de Huaynacotas, provincia de La Unión, departamento de Arequipa **505514**

Res. N° 950-2013-JNE.- Restablecen la vigencia de credencial otorgada a alcalde de la Municipalidad Distrital de Cuchumbaya, provincia de Mariscal Nieto, departamento de Moquegua **505515.**

3.15.- Ministerio publico.

Res. N° 152-2013-MP-FN-JFS.- Crean Fiscalías Especializadas en Delito de Lavado de Activos y Pérdida de Dominio con competencia nacional, conformadas por Fiscalías Superiores Nacionales y Fiscalías Supra provinciales Corporativas Especializadas, con sede en Lima **505516 RR. N°s. 3429 y 3430-2013-MP-FN.-** Dan por concluido nombramiento y nombran fiscales provisionales en el Distrito Judicial de Lima **505517**

3.16.- superintendencia de banca, seguros y administradoras privadas de fondos de pensiones.

Res. N° 6201-2013.- Autorizan a la Edpyme Inversiones La Cruz S.A. la apertura de agencias en los departamentos de Lima, Ucayali y Piura **505518.**

CAPITULO IV

JURISPRUDENCIAS

4.1 exp n ° 00108 2014-pa/tc loreto alexci igor chong ríos Sentencia interlocutoria del tribunal constitucional Lima, 4 de marzo de 2016.

ASUNTO

Recurso de agravio constitucional interpuesto por don Alexci Igor Chong Ríos contra la resolución de fojas 114, su fecha 19 de agosto de 2013, expedida por la Sala Civil Mixta de Maynas de la Corte Superior de Justicia de Loreto, que declaró improcedente la demanda de autos.

Tribunal constitucional

EXP N ° 00108 2014-PA/TC LORETO ALEXCI IGOR CEIONG RÍOS SENTENCIA INTERLOCUTORIA DEL TRIBUNAL CONSTITUCIONAL Lima, 4 de marzo de 2016.

Asunto:

Recurso de agravio constitucional interpuesto por don Alexci Igor Chong Ríos contra la resolución de fojas 114, su fecha 19 de agosto de 2013, expedida por la Sala Civil Mixta de Maynas de la Corte Superior de Justicia de Loreto, que declaró improcedente la demanda de autos.

Fundamentos

1. En la sentencia emitida en el Expediente 00987-2014-PA/TC.

Publicada en el diario oficial *El Peruano* el 29 de agosto de 2014, este Tribunal estableció, en el fundamento 49, con carácter de precedente, que se expedirá sentencia interlocutoria denegatoria, dictada sin más trámite, cuando concurra alguno de los siguientes supuestos que, igualmente, están contenidos en el artículo 11 del Reglamento Normativo del Tribunal Constitucional, los cuales se presentan cuando:

a) Carezca de fundamentación la supuesta vulneración que se invoque.

b) La cuestión de Derecho contenida en el recurso no sea de especial trascendencia
constitucional.

c) La cuestión de Derecho invocada contradiga un precedente del Tribunal Constitucional.

d) Se haya decidido de manera desestimatoria en casos sustancialmente iguales.

2. En el presente caso, se evidencia que el recurso de agravio no está referido a una cuestión de derecho de especial trascendencia constitucional. Al respecto, un

recurso carece de esta cualidad cuando no está referido al contenido constitucionalmente protegido de un derecho fundamental; cuando versa sobre un asunto materialmente excluido del proceso de tutela de que se trata; o, finalmente, cuando lo pretendido no alude a un asunto que requiere una tutela de especial urgencia.

3. Expresado de otro modo, y teniendo en cuenta lo precisado en el fundamento 50 de la sentencia emitida en el Expediente 00987-2014-PA/TC, una cuestión no reviste
especial trascendencia constitucional en los siguientes casos: si una futura resolución del Tribunal Constitucional no soluciona algún conflicto de relevancia constitucional, pues no existe lesión de derecho fundamental comprometida.

trata de un asunto que no corresponde ser resuelto en la vía constitucional; si no existe necesidad de tutelar de manera urgente el derecho constitucional invocado, sin que medien razones subjetivas u objetivas que habiliten a este órgano
colegiado a emitir un pronunciamiento de fondo.

4. En efecto, el presente recurso no está referido a una cuestión de Derecho de especial trascendencia constitucional, en vista de que se encuentra inmerso en el primer supuesto señalado en el fundamento precedente (trata de un asunto que no corresponde resolver en la vía constitucional). Y es que si bien la parte demandante alega haber sido víctima de un despido fraudulento, existen hechos controvertidos que solo pueden ser resueltos mediante la actuación de medios probatorios, ya que los medios obrantes en autos son insuficientes y contradictorios, de conformidad con el artículo 9 del Código Procesal Constitucional.

5. En el caso de autos, el demandante alega que los hechos imputados, acaecidos el 4 de marzo de 2013, son falsos, pues nunca se le otorgó, asignó o recibió en custodia el indicado PC, de nombre LIGEP-P-03, con dirección IP 192.162.1.59, así como un escritorio y otros útiles, más aún cuando no hay un acta de constatación de entrega y/o recepción de bienes de trabajo, de conformidad con los instrumentales obrantes a fojas 46, 56, 57 y 70. Asimismo, refiere que dichos actos responden a una represalia por su condición de dirigente sindical (secretario general) por el periodo 2013-2015 (ff. 30 - 42), lo cual se evidencia cuando solicitó licencia sindical.

6. Por otro lado, a fojas 69 de autos, obra el Informe de verificación de equipo de cómputo, de fecha 4 de marzo de 2013, el cual contiene la supuesta firma del ahora recurrente, y en donde se constató que en la PC de nombre LIGEP-P-03, con dirección IP 192.162.1.59, asignado al señor Alexci Igor Chong Ríos, se encontró instalado el software de nombre Ultrusurf, cuya principal función es vulnerar la políticas de seguridad de navegación de internet del Firewall, haciendo que este sea libre y de total acceso sin restricciones, lo cual implicaría que el actor incurrió en las faltas graves tipificadas en los incisos a) y c) del artículo 25 del Decreto Supremo 003-97-TR y en el artículo 55 del Reglamento Interno de Trabajo de la emplazada, tal como se aprecia de los medios probatorios obrantes a fojas 43, 53 y 54.

7. De lo expuesto, esta Sala del Tribunal estima que no es posible verificar con certeza si el actor cometió o no las faltas graves imputadas, o si, por el contrario, son hechos falsos que responden a una represalia por su actividad sindical, por lo que no obrar instrumentales adicionales, el proceso de amparo no resulta idóneo para dilucidar la controversia vertida.

Publíquese y notifique \SS. Ramos núñez espinosa-s bar Tribunal constitucional Exp n.° 00108 2014-pa/tc Loreto - Alexci igor chong ríos.

8. Sin perjuicio de lo expuesto, debe indicarse que si bien la empresa Electro Oriente S.A. formuló denuncia contra el ahora actor y otro por el delito de intrusismo informático, Carpeta Fiscal 2506014507-2013-448-0, donde se resolvió formalizar y continuar investigación preparatoria en la vía del proceso común, por la presunta comisión de delito contra el patrimonio - delitos informáticos en la modalidad de delito de intrusismo informáticos (f. 143), mediante Resolución N.° 3, de fecha 27 de marzo de 2014, el Segundo Juzgado Penal de Investigación Preparatoria de Iquitos emitió el auto de sobreseimiento de dicha denuncia por considerar que en el caso del señor Alexci Igor Chong Ríos no se contaba con suficientes elementos para solicitar
fundadamente su enjuiciamiento (f. 21 del cuadernillo del Tribunal Constitucional). Dicha resolución fue declarada consentida mediante resolución de fecha 20 de junio de 2014 (f. 44 del referido cuadernillo).

9. En consecuencia, y de lo expuesto en los fundamentos 2 a 8 *supra*, se verifica que el presente recurso de agravio ha incurrido en la causal de rechazo prevista en el acápite b) del fundamento 49 de la sentencia emitida en el Expediente 00987-2014- PA/TC y en el inciso b) del artículo 11 del Reglamento Normativo del Tribunal Constitucional. Por esta razón, corresponde declarar, sin más trámite, improcedente el recurso de agravio constitucional.

Por estos fundamentos, el Tribunal Constitucional, con la autoridad que le confiere la
Constitución Política del Perú.

Resuelve:

Declarar IMPROCEDENTE el recurso de agravio constitucional porque la cuestión de Derecho contenida en el recurso carece de especial trascendencia constituye I. Juan Otarola Santillana Secretaria Re1atora Tribunal constitucional zonal.

4.2.- Sentencia del tribunal constitucional exp. N.o 02022-2008-phc/tc En Lima, (Arequipa) a los 22 días del mes de setiembre de 2008, la Sala Primera del Tribunal Con:!itucional, integrada por los Magistrados Landa Arroyo, Beaumont Callirgos y Eto Cruz.

4.3.- Sentencia del 33º Juzgado Penal de Lima. Corte Superior de Justicia de Lima. Resolución nº 21 de 29 octubre 2010, Expediente 24304-2009-0-1801-JR-PE-33, Caso José Alejandro Godoy Mejía. Especialista: Rivera Orrego, Marco Antonio. Querellado:

Godoy Mejía, José Alejandro. Delito: Difamación a través de blog. Querellante: Mufarech Nemy, Jorge Yamil.

CAPITULO V

DERECHO COMPARADO

5.1 .- Consideraciones generales del derecho informático en la legislación comparada

El análisis internacional y/o regional de los delitos informáticos es de gran dificultad porque por definición, el Derecho Penal es todavía prominentemente un asunto de carácter nacional. A pesar de que existe un creciente movimiento para crear Principios De Derecho Penal Internacional, no se ha llegado todavía a desarrollar un concepto o internacional de delitos informáticos, por lo que este tema debe ser estudiado por ahora en la forma que se presenta en cada país. Esta situación se hace más clara cuando se toma en cuenta que distintos sistemas jurídicos conllevan diferencias a la hora de criminalizar una acción. En sistemas civiles, para poder tipificar un delito hay que establecer cuál es el bien jurídico que la sociedad quiere proteger, y de él desprender cuales serían los hechos punibles, en caso de que dicho bien jurídico sea vulnerado, y establecer por ende cual es la pena por vulnerar dicho bien jurídico. En sistemas de derecho común, no existe codificación de delitos, y los tipos pueden hasta ser el resultado de costumbre o jurisprudencia.

La dificultad de poder realizar una sistematización adecuada se evidencia asimismo por la gran diversidad de delitos y bienes jurídicos protegidos. Los Estados

Unidos proveen un excelente ejemplo de la gran variedad de delitos relacionados con las TIC. Por ejemplo, existen Estados con diversos delitos que no se encuentran en otros, y hasta ahora se ha criminalizado ciertos tipos de correos basura o Spam. Esto se da mientras en otros países se encuentra la tipificación de prohibir el uso de juegos de computadora en cafés de Internet. El asunto tan complejo que la misma Unión Europea se ha despreocupado casi totalmente del tema de las TIC

y el Derecho penal, pero no de manera completa ya que se ha publicado un Convenio sobre Cibercriminalidad, el cual no tiene carácter obligatorio para estados miembros, y tan solo ha sido ratificado por 5 países; sin embargo, en medio de esta gran variedad de tipos penales, se pueden empezar a ver algunas tendencias que permiten un limitado análisis comparativo. Inicialmente, se puede decir que existe un creciente número de delitos tipificados que pueden ser utilizados en casos que se relacionen con TIC, pero dependerá de la pericia jurídica en demostrar que las TIC fue el medio mas no el fin en sí misma de los delitos. Tal es el caso de difamación, el hecho que sea por medios informáticos no hace que sea otro delito, sino que resultaría que el uso de las TIC configure un agravante o un medio para la realización del delito. Lo mismo ocurriría en el caso de un fraude o delitos de apología del delito. Muchos de estos "delitos mediante medios digitales", se encontrarían ya tipificados en los códigos penales existentes. En realidad quizás uno de los problemas mayores no esté en la tipificación de los delitos sino en determinar la legislación y la jurisdicción aplicable (cuando la misma es extra-territorial).

Con el advenimiento de los procesos de Sociedad de la Información, la aparición de nuevos escenarios, nuevas inter-relaciones y nuevas "etiquetas" para las conductas han generado que se trate de regular aquellos actos que vulnerarían derechos. De esta manera apareciera el concepto de *Delitos Informáticos*, que en sentido estricto son aquellos delitos que afectan al bien jurídico "información" (en cualquiera de sus formas: desde mensajes de datos hasta sistemas computacionales); frente a los *Delitos por medios informáticos* que serían una actualización de los delitos ya tipificados pero con un nuevo medio: el tecnológico.

Bajo esta premisa inicial se comenzó a desarrollar las formas de perseguir dichos delitos, y dichas formas, basándose en el principio jurídico de "no hay pena si no hay ley", requerían la tipificación y explicitación de los hechos delictivos.

En cierta manera los delitos por medios informáticos son variantes de los delitos "clásicos", por lo cual muchos legisladores optaron por el camino de adecuación normativa, es decir colocar en los artículos pertinentes la acepción "... Y por medios electrónicos", o similares.

Es por ejemplo el caso en el Código Penal de el Salvador o la modificatoria al Código Penal Chileno. En otros casos se planteó la posibilidad de la inclusión de un artículo en la parte general de los códigos penales que sea genérica, indicando que el hecho que sea utilizando alguna TIC agravaría el hecho. Este cambio de adecuación normativa afectaba en esencia a un código penal ya existente.

Pero las actividades relacionadas a intrusismo informático, sabotaje informático y en General aquellas que afectarán a la información, no se encontrarían contempladas puesto que no encuadran, alguno de los delitos Pre-existentes a la irrupción de las TIC. En sentido estricto a estos se les debe denominar Delitos Informáticos. El camino que siguieron los legisladores fue el desarrollo que normas específicas (el caso particular de Venezuela y Chile que son leyes específicas separadas del código penal), el desarrollo de normas específicas que insertaban artículos en el Código Penal, como el caso de Perú, o normas relacionadas que modificaban el Código Penal (el caso de la ley De Protección De Datos de Argentina o la ley de Comercio Electrónico de Ecuador).

5.2.- Las fuentes del derecho informático en el derecho comparado.

a) Los Tratados

Barberis define como Tratado "una manifestación de voluntad común de dos o más sujetos de derecho de gentes con capacidad suficiente, tendiente a establecer una regla de derecho en el orden jurídico internacional y que está regida directamente por este ordenamiento."

El concepto expresado es amplio, y en él quedan comprendidos no sólo los denominados Tratados, sino también Convenciones, como las que se mencionarán.

Observa que el Tratado es una regla de derecho válida, que se encuentra directamente regida por el derecho de gentes, tendiente a modificar una situación jurídica existente o a definir ciertos conceptos. Pueden ser nulos en tanto no cumplan con las características de los Tratados, antes establecidas en la definición. Tanto los Tratados como las Resoluciones y demás manifestaciones escritas poseen cierta dosis de indeterminación o vaguedad por estar escritas en lenguaje natural, denominado de "textura abierta", por lo que se habla de la "textura abierta del Derecho", según Barberis.; en la contratación electrónica internacional, salvo las previsiones expresas en la materia específica, y respecto a los Estados firmantes y aquellos que las incorporen a la legislación interna de cada país posteriormente, resultan fuentes de Derecho subsidiarias, las Convenciones Internacionales referidas a los contratos, las Convenciones emanadas de las conferencias de La Haya, (convención sobre la ley aplicable a las ventas de carácter internacional de objetos muebles corporales, de 15 de junio de 1955, convención sobre la ley y aplicable a la transferencia de la propiedad en ventas internacionales de bienes muebles corporales de aprobada en abril de 1958, la que regula la competencia fin igual materia, de la misma fecha, la ley uniforme sobre compraventas internacionales de 1964, sobre formación del contrato de compraventa internacional también de 1964, y ley aplicable en igual tipo contractual de 1986).

Más recientemente, de los trabajos de las Naciones Unidas han surgido la convención sobre la prescripción en materia de compraventa internacional de mercaderías (N. York 14.6. 1974) enmendada por el protocolo de 11.4. 1980, El Convenio De Las Naciones Unidas Sobre Transporte Marítimo De Mercancías De 1978 (Reglas de Hamburgo), la Convención De Las Naciones Unidas Sobre Los Contratos De Compraventa Internacional De Mercancías (Viena, 1980), la convención de Roma sobre la ley aplicable a las obligaciones contractuales internacionales aprobadas el 19 de junio de 1980, las Convenciones Relativas A Letras De Cambio Internacionales, Pagarés Internacionales, Responsabilidad De Empresarios De Terminales De Transporte En El Comercio Internacional, Garantías Y Cartas De Crédito Contingente, Y Las Referidas Arbitraje Comercial Internacional Y Reconocimiento Y Ejecución De Las Sentencias Arbitrales Extranjeras.

En el área de los Estados Americanos y desde la OEA, de la labor de conferencias especializadas en Derecho Internacional Privado (CIDIP), surge en elaboraciones como la convención de 1994 aprobada en México, relativa a derecho aplicable a la contratación internacional. En el área del MERCOSUR, es aplicable el protocolo del MERCOSUR sobre Jurisdicción En Materia Contractual. La validez de toda esta normativa queda supeditada a la internalización mediante ley en cada país.

b) La Costumbre

La costumbre es otra fuente del Derecho Internacional de gran trascendencia, antecedente de muchos Tratados y de carácter predominante en la formación de esta rama del Derecho, conservándose normas consuetudinarias en cuanto a responsabilidad internacional, protección diplomática y procedimiento arbitral hasta hoy, según el mismo Barberis, siendo la fuente de solución de los problemas nuevos.

Las normas consuetudinarias adolecen de mayor imprecisión que los tratados o resoluciones, expresados en lenguaje escrito, consiste, según algunos autores en la manifestación de un derecho ya existente (*Volksgeist, droitobjectif)* del que constituye una comprobación, en una fuente de Derecho Internacional que se

considera un tratado tácito o un método de creación de Derecho, siendo para otros un Derecho espontáneo que no tiene una forma específica de creación.

Las normas consuetudinarias se identifican como tales si reúnen dos factores: el elemento material: la práctica y otro denominado la "opinio juris sive necessitates" u " opinio iuris", concepto polémico originado en el siglo XIX y desarrollado por la escuela historisista alemana, que es" la convicción que han de tener los sujetos que realizan una práctica, de observarla como si se tratara de una norma jurídica", como si fuera obligatoria, como la convicción de que se origina en una norma de derecho que los sujetos creen como existente, o convencidos de la necesidad de observar cierto uso o práctica determinada, o de que la observan como un deber impuesto por la moral, la justicia o el derecho natural, según las distintas opiniones. La noción de opinio iuris se entiende comprendida en parte de la definición de costumbre del artículo 38, inciso 1°, b, Del Estatuto Del Tribunal De La Haya; la convención de Viena de 1980, (ratificada por 59 Estados), que no contiene ninguna regla imperativa, se refiere a la obligación de las partes de respetar los usos y prácticas que hayan convenido y " cualquier uso que se ha ampliamente conocido y regularmente observado en el tráfico mercantil de que se trate" con la excepción de los usos que no sean razonables, con lo cual se genera el problema de saber cuál es el uso razonable, que podrá dilucidarse en la vía arbitral o judicial; como expresa Diego Galante Álvares, quien menciona en ese sentido a weiss, " debe distinguirse la costumbre internacional de la interna; expresa que " la primera es una convención tácita ratificada por la tradición" que " se forma por el consentimiento presunto de las naciones interesadas", mientras que la segunda " se forma por una disposición presunta de la autoridad encargada de dictarla" expresa que " habría... Costumbres de Derecho Internacional Público aplicables a determinados problemas de Derecho Internacional Privado", " aún cuando sea criticado la carencia de sanciones efectivas a los transgresores de la costumbre internacional" dentro de este último.

El tema es relevante en cuanto a la contratación informática y a los modelos de contratos en especial, dado que en la normativa interna de muchos países no existe

regulación específica, o resulta parcial y dispersa, por lo que en la práctica se recurre a modelos de la normativa internacional, como los modelos de CNUDMI oo de la Comunidad Europea, fuentes de inspiración además, de la legislación que se viene creando en los diferentes países.

c) Las Prácticas

En cuanto a la práctica, requiere la repetición de actos humanos o abstenciones, de cierta generalidad, observados en forma ininterrumpida y constante en un determinado ámbito espacial. Los sujetos que deben realizar la práctica pueden ser órganos internos o externos de los Estados, organizaciones y tribunales internacionales. En este último caso un ejemplo lo constituyen las reglas principales que son la base del procedimiento arbitral, que han sido establecidas en la práctica de los tribunales, como la que otorga a un tribunal la facultad de dictar medidas precautorias, creada por la jurisprudencia internacional, o aquella según la cual "una parte no puede oponer a la otra el hecho de no haber cumplido una obligación o no haber interpuesto un recurso procesal si la primera, mediante un acto contrario al derecho, ha impedido a esta última cumplir la obligación o interponer el recurso".

En el Derecho Informático, Las Prácticas Y Códigos De Prácticas tienen gran relevancia en temas claves como los Nombres De Dominios, cuya adjudicación la regula la Corporación Internacional ICANN (Internet Corporation For Assigned Names And Numbers), mediante la aplicación de códigos de práctica, que la misma organización elabora, y que establecen reglas para la adjudicación de las direcciones de internet, la organización de los números y nombres de dominio y los estándares para los protocolos de funcionamiento de internet, esta organización reúne en sí la potestad legislativa, administrativa y judicial ya que elabora las normas y las aplica a los casos concretos.

En la especifica materia contractual, las prácticas y códigos de prácticas tienen gran relevancia como Fuente Del Derecho Informático, en cuanto a un aspecto clave como es la seguridad, material y formal, la criptografía, tema que será objeto de otro

punto de este trabajo. También se encuentran establecidas por Organizaciones Internacionales en este caso, la O.C.D.E.

CAPITULO VI

CONCLUSIONES

1) La incursión de la informática en todos los niveles de las ciencias, está cambiando las viejas formas de pensar en la medicina, astronomía, contabilidad, y por supuesto en la ciencia jurídica, prueba de ello es que nuestra normatividad incluye en su catálogo de delitos los vinculados a la informática, como forma de proteger el bien jurídico que esta representa.

2) Actualmente, los operadores del Derecho valoran adecuadamente las pruebas aportadas al proceso penal por la comisión de delitos informáticos, sin que con dicha valoración se afecten derechos fundamentales de las personas.

3) Los resultados pragmáticos del derecho informático en aplicación al Derecho Penal se advierte en las normativas de protección de datos personales que han sido creadas con el propósito de evitar atentados contra la privacidad de las personas, ante la inminente aparición de diversas formas tecnológicas.

4) No obstante lo concluido en el punto anterior, en el caso peruano la constelación normativa con la que contamos es muy incipiente respecto a éstos fenómenos, lo que amerita cambios sustanciales en el marco legal

imperante y sobre todo el que se voten normas que regulen más eficiente e integralmente, ésta revolución informática.

CAPITULO VII

RECOMENDACIONES

Si partimos de la premisa de que existe un principio jurídico que señala que “no hay pena sin ley previa”, queda claro que toda acción antijurídica debe estar correctamente tipificada como delito para poder sancionarla, por ello, las tareas pendientes están enfocadas a establecer un lenguaje común para poder integrar las propuestas posibles a la normativa local.

1) Es necesario unificar y sistematizar el Derecho Informático, en un cuerpo ordenado de normas, a efecto de darle independencia y autonomía como rama de la ciencia jurídica.

2) Se debe deslindar toda confusión terminológica entre lo que son delitos informáticos y delitos por medios electrónicos, siendo tarea fundamental el establecer una adecuada diferenciación y por ende regulación donde se requiera en base a la diferencia conceptual. Asimismo, debe ir acompañado del diseño de una propuesta normativa mínima, basada entre otros, en las propuestas de tratados de Cybercrimen, ya existentes.

3) Se requiere capacitar al Poder judicial, Policía Nacional y todos aquellos que realizan investigaciones relevantes a causas penales en temas de aspectos legales de Sociedad de la Información, así como formarlos en las herramientas necesarias para combatir estos ilícitos.

4) Se debe desarrollar una propuesta regional que permita interactuar a los actores jurídicos de una manera transfronteriza respetando la legislación y jurisdicción propia de cada uno de los países.

CAPÍTULO VIII

RESUMEN

En los tiempos actuales, se le ha tenido a bien denominar “sociedad de la información” por el vertiginoso desarrollo científico y tecnológico que implica el avance de la informática en las diversas esferas del quehacer político, económico y social a escala mundial y, recordando que la informática es entendida como la disciplina o actividad que consiste en el tratamiento o procesamiento de la informática por medio de máquinas ordenadoras electrónicas tendientes a la obtención de nueva información ; cuyo uso inadecuado y sin control puede volverse en contra del mismo hombre creador de la tecnología, invadiendo las esferas más íntimas de su vida privada.

La regulación de las nuevas tecnologías de la información y la comunicación en sí conlleva a la necesidad de reflexionar sobre la función del derecho en sus diferentes ramas como en el derecho Penal, Respecto a la informática necesitamos recurrir a ella para conocer cuáles son las conductas que la comunidad científica-tecnológica considera que deben protegerse por el Derecho, mientras que el Derecho debe indagar qué es el delito para posteriormente cuestionar si la utilización masiva de las computadoras u ordenadores y la telemática pueden cambiar la naturaleza y alcance de la ley penal.

CAPITULO IX

REFERENCIAS BIBLIOGRÁFICAS

- ✓ Blossiers, juan. 2003-criminalidad informática,(1era, ed.). Lima ed. Librería portocarreo s.r.l. p. 225; 152; 153; 155; 160-163.

- ✓ Comercio electrónico en internet, marcial pons, madrid 2001.

- ✓ Davara, miguel 2004. Manual de derecho informático(6ta. Ed.), navarra,ed.aranzadi s.a. pp. 46; 28; 348; 350.

- ✓ Diario el peruano.

- ✓ Elliot segura, aldo antonio. La proteccion del dercho a la intimidad y privacidad frente a las nuevas tecnologías, en revista del vii congreso iberoamericano de derecho e informática, editora perú, lima 2000.

- ✓ Enciclopedia microsoft en carta telemática, edición 2007.

- ✓ Espino gonzales miguel. La justicia y la máquina, ediciones panamá.

- ✓ Eugenio, francisco. Informatización del dercho, universidad, computacion y derecho; sobre sus implicasiones reciprocas informática y derecho.

- ✓ Ferreyros soto, carlos. Globalización e informática jurídica: el derecho del notariado, revista del vii congreso iberoamericano de derecho e informática, editora perú 2000.

- ✓ García cantizado,falsedades documentales,ed.tirantlo blach, valencia 1994, ps. 178-179.

- ✓ García cantizano, o.u.c. ps. 163 y ss.

- ✓ Garza mercado, ario. Las ciencias de la información en la escuela de bibliotecologia, citado por amat noguera,nuria. Técnicas documentales y fuentes de información.

- ✓ Gobierno del perú: constitución política el perú. Lima.ed. Miguel ramos b.p.31.

- ✓ Gomez segade, josé. "el comercio electrónico en las sociedade de la informació" en: gomez segade, josé (dir).

- ✓ Guerreo m., maría fernanda. La inteligencia artificial aplicada al derecho, revista uno y cero, milán.

- ✓ Guisado moreno, ángela. La formación y perfección del contrato en internet, marcial pons, madrid 2004.

- ✓ Gutierres frances, fraude informático y estafa, op. Cit, p. 134.

- ✓ Gutierres frances,o.u.c.,p.125.
- ✓ Https://alicia.concytec.gob.pe/.
- ✓ Http://es.wikipedia.org/wiki/derecho,(consultado el 20 de junio 2014).
- ✓ Romero luis.2005 tesis ;marco conceptual de los delitos informáticos, lima, unmsm, p. 2.
- ✓ Sueber,criminalidad informática,op.cit.p,25.
- ✓ Tiedemann, poder económico y delito, op. Cit, p. 126-127.
- ✓ Url: http://www.npros.com.pe/new/pq=cursos.
- ✓ Wikipedia, información sobre el derecho.
- ✓ Wikipedia, informática.

CAPÍTULO X

ANEXOS

TRIBUNAL CONSTITUCIONAL

EXP. N.° 00108-2014-PA/TC
LORETO
ALEXCI IGOR CHONG RÍOS

SENTENCIA INTERLOCUTORIA DEL TRIBUNAL CONSTITUCIONAL

Lima, 4 de marzo de 2016

ASUNTO

Recurso de agravio constitucional interpuesto por don Alexci Igor Chong Ríos contra la resolución de fojas 114, su fecha 19 de agosto de 2013, expedida por la Sala Civil Mixta de Maynas de la Corte Superior de Justicia de Loreto, que declaró improcedente la demanda de autos.

FUNDAMENTOS

1. En la sentencia emitida en el Expediente 00987-2014-PA/TC, publicada en el diario oficial *El Peruano* el 29 de agosto de 2014, este Tribunal estableció, en el fundamento 49, con carácter de precedente, que se expedirá sentencia interlocutoria denegatoria, dictada sin más trámite, cuando concurra alguno de los siguientes supuestos que, igualmente, están contenidos en el artículo 11 del Reglamento Normativo del Tribunal Constitucional, los cuales se presentan cuando:

   a) Carezca de fundamentación la supuesta vulneración que se invoque.
   b) La cuestión de Derecho contenida en el recurso no sea de especial trascendencia constitucional.
   c) La cuestión de Derecho invocada contradiga un precedente del Tribunal Constitucional.
   d) Se haya decidido de manera desestimatoria en casos sustancialmente iguales.

2. En el presente caso, se evidencia que el recurso de agravio no está referido a una cuestión de derecho de especial trascendencia constitucional. Al respecto, un recurso carece de esta cualidad cuando no está referido al contenido constitucionalmente protegido de un derecho fundamental; cuando versa sobre un asunto materialmente excluido del proceso de tutela de que se trata; o, finalmente, cuando lo pretendido no alude a un asunto que requiere una tutela de especial urgencia.

3. Expresado de otro modo, y teniendo en cuenta lo precisado en el fundamento 50 de la sentencia emitida en el Expediente 00987-2014-PA/TC, una cuestión no reviste especial trascendencia constitucional en los siguientes casos: (1) si una futura resolución del Tribunal Constitucional no soluciona algún conflicto de relevancia constitucional, pues no existe lesión de derecho fundamental comprometida o se

trata de un asunto que no corresponde ser resuelto en la vía constitucional; o, (2) si no existe necesidad de tutelar de manera urgente el derecho constitucional invocado, sin que medien razones subjetivas u objetivas que habiliten a este órgano colegiado a emitir un pronunciamiento de fondo.

4. En efecto, el presente recurso no está referido a una cuestión de Derecho de especial trascendencia constitucional, en vista de que se encuentra inmerso en el primer supuesto señalado en el fundamento precedente (trata de un asunto que no corresponde resolver en la vía constitucional). Y es que si bien la parte demandante alega haber sido víctima de un despido fraudulento, existen hechos controvertidos que solo pueden ser resueltos mediante la actuación de medios probatorios, ya que los medios obrantes en autos son insuficientes y contradictorios, de conformidad con el artículo 9 del Código Procesal Constitucional.

5. En el caso de autos, el demandante alega que los hechos imputados, acaecidos el 4 de marzo de 2013, son falsos, pues nunca se le otorgó, asignó o recibió en custodia el indicado PC, de nombre LIGEP-P-03, con dirección IP 192.162.1.59, así como un escritorio y otros útiles, más aún cuando no hay un acta de constatación de entrega y/o recepción de bienes de trabajo, de conformidad con los instrumentales obrantes a fojas 46, 56, 57 y 70. Asimismo, refiere que dichos actos responden a una represalia por su condición de dirigente sindical (secretario general) por el periodo 2013-2015 (ff. 30 - 42), lo cual se evidencia cuando solicitó licencia sindical.

6. Por otro lado, a fojas 69 de autos, obra el Informe de verificación de equipo de cómputo, de fecha 4 de marzo de 2013, el cual contiene la supuesta firma del ahora recurrente, y en donde se constató que en la PC de nombre LIGEP-P-03, con dirección IP 192.162.1.59, asignado al señor Alexci Igor Chong Rios, se encontró instalado el software de nombre Ultrusurf, cuya principal función es vulnerar las políticas de seguridad de navegación de internet del Firewall, haciendo que este sea libre y de total acceso sin restricciones, lo cual implicaría que el actor incurrió en las faltas graves tipificadas en los incisos a) y c) del artículo 25 del Decreto Supremo 003-97-TR y en el artículo 55 del Reglamento Interno de Trabajo de la emplazada, tal como se aprecia de los medios probatorios obrantes a fojas 43, 53 y 54.

7. De lo expuesto, esta Sala del Tribunal estima que no es posible verificar con certeza si el actor cometió o no las faltas graves imputadas, o si, por el contrario, son hechos falsos que responden a una represalia por su actividad sindical, por lo que no obrar instrumentales adicionales, el proceso de amparo no resulta idóneo para dilucidar la controversia vertida.

TRIBUNAL CONSTITUCIONAL

EXP. N.° 00108-2014-PA/TC
LORETO
ALEXCI IGOR CHONG RÍOS

8. Sin perjuicio de lo expuesto, debe indicarse que si bien la empresa Electro Oriente S.A. formuló denuncia contra el ahora actor y otro por el delito de intrusismo informático, Carpeta Fiscal 2506014507-2013-448-0, donde se resolvió formalizar y continuar investigación preparatoria en la vía del proceso común, por la presunta comisión de delito contra el patrimonio - delitos informáticos en la modalidad de delito de intrusismo informáticos (f. 143), mediante Resolución N.° 3, de fecha 27 de marzo de 2014, el Segundo Juzgado Penal de Investigación Preparatoria de Iquitos emitió el auto de sobreseimiento de dicha denuncia por considerar que en el caso del señor Alexci Igor Chong Rios no se contaba con suficientes elementos para solicitar fundadamente su enjuiciamiento (f. 21 del cuadernillo del Tribunal Constitucional). Dicha resolución fue declarada consentida mediante resolución de fecha 20 de junio de 2014 (f. 44 del referido cuadernillo).

9. En consecuencia, y de lo expuesto en los fundamentos 2 a 8 *supra*, se verifica que el presente recurso de agravio ha incurrido en la causal de rechazo prevista en el acápite b) del fundamento 49 de la sentencia emitida en el Expediente 00987-2014-PA/TC y en el inciso b) del artículo 11 del Reglamento Normativo del Tribunal Constitucional. Por esta razón, corresponde declarar, sin más trámite, improcedente el recurso de agravio constitucional.

Por estos fundamentos, el Tribunal Constitucional, con la autoridad que le confiere la Constitución Política del Perú,

RESUELVE

Declarar **IMPROCEDENTE** el recurso de agravio constitucional porque la cuestión de Derecho contenida en el recurso carece de especial trascendencia constitucional.

Publíquese y notifíquese.

SS.

URVIOLA HANI
RAMOS NÚÑEZ
ESPINOSA-SALDAÑA BARRERA

Lo que certifico:

JANET OTÁROLA SANTILLANA
Secretaria Relatora
TRIBUNAL CONSTITUCIONAL