UNIVERSIDAD PRIVADA SAN CARLOS

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE DERECHO

TESIS

EL DELITO CONTRA DATOS INFORMÁTICOS PERSONALES EN EL DERECHO FUNDAMENTAL A LA INTIMIDAD PERSONAL EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2020

PRESENTADO POR:

MARIA ELENA CCAMA CENTENO

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

PUNO – PERÚ

2021

UNIVERSIDAD PRIVADA SAN CARLOS

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE DERECHO

TESIS

EL DELITO CONTRA DATOS INFORMÁTICOS PERSONALES EN EL DERECHO FUNDAMENTAL A LA INTIMIDAD PERSONAL EN LA CORTE SUPERIOR DE JUSTICIA PUNO 2020

PRESENTADO POR:

MARIA ELENA CCAMA CENTENO

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADO

APROBADO POR EL SIGUIENTE JURADO:

PRESIDENTE : _____
DR. BENITO PEPE CALSINA CALSINA

PRIMER MIEMBRO : _____
MSC. DENILSON MEDINA SANCHEZ

SEGUNDO MIEMBRO : _____
MSC. MARTIN WILLIAM HUISA HUAHUASONCCO

ASESOR DE TESIS : _____
MGTR. PERCY GABRIEL MAMANI PUMA

Área: Ciencias Sociales

Disciplina: Derecho Público

Especialidad: Derecho Penal y procesal penal

Puno, 13 de Octubre del 2021

DEDICATORIA

“Quiero dedicar esta tesis de grado a Dios por permitirme culminar con éxito mi tan anhelada carrera, darme buena salud y fortaleza en todo momento, también dedico este trabajo con gran amor a toda mi familia por el apoyo incondicional, por siempre impulsarme a ser mejor y lograr con éxito mi carrera”.

AGRADECIMIENTO

“Gracias a la Universidad Privada San Carlos, casa de estudio que me permitió crecer académicamente y tener una educación de calidad. A los valiosos docentes que me impartieron sus conocimientos y me ayudaron en cada paso que di”.

ÍNDICE GENERAL

CAPÍTULO II

MARCO TEÓRICO, CONCEPTUAL E HIPÓTESIS DE LA INVESTIGACIÓN

CAPÍTULO IV

METODOLOGÍA DE LA INVESTIGACIÓN

CAPÍTULO IV

EXPOSICION Y ANALISIS DE LOS RESULTADOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

RESUMEN

La presente investigación actual adopta un enfoque del derecho a la privacidad desde el punto de vista de su regulación y aplicación en el sistema legal peruano con respecto a sus deficiencias. Esta razón fundamental ahora se considera uno de los más vulnerables en forma directa e indirecta por medio de las redes sociales que incluye un aumento masivo entre las personas.

El mundo digital representa como un fenómeno de los nuevos tiempos que estamos viviendo hoy en día, donde la investigación aborda el problema que existe en la falta de protección penal de la intimidad personal en el uso de las redes sociales donde se esta volviendo más accesible en el Perú, en tal sentido es donde se hace una descripción de la realidad problemática y a consecuencia de ello se formula en forma de interrogante los problemas generales y los específicos, a partir de las interrogantes, es donde se determinan los objetivos, por los cuales se podrán guiar la investigación.

El marco teórico, comienza con los diferentes delitos informáticos y con los derechos a la intimidad en los que puede afectar, y otros temas de gran importancia, conforme al problema que se va presentando, haciendo el uso de la información tanto física como virtual que respalden a nuestra investigación.

De la misma manera se usó la metodología de investigación más adecuada, que nos ayude no solo a describir y profundizar el problema, también realizar la descripción de manera más coherente la información analizada, la investigación finaliza, con las conclusiones y recomendaciones.

Palabras clave: Delitos, Datos Informáticos, Derecho Fundamental, Intimidad Personal, Corte Superior de Justicia

ABSTRACT

The present current research adopts an approach to the right to privacy from the point of view of its regulation and application in the Peruvian legal system with respect to its deficiencies. This rationale is now considered one of the most vulnerable directly and indirectly through social media which includes a massive increase among people.

The digital world represents as a phenomenon of the new times that we are living today, where research addresses the problem that exists in the lack of criminal protection of personal privacy in the use of social networks where it is becoming more accessible in Peru, in this sense, is where a description of the problematic reality is made and as a result, the general and specific problems are formulated in the form of a question, based on the questions, it is where the objectives are determined, by which the they will be able to guide the investigation.

The theoretical framework begins with the different computer crimes and with the rights to privacy in which it can affect, and other issues of great importance, according to the problem that arises, making use of both physical and virtual information that support to our investigation.

In the same way, the most appropriate research methodology was used, which helps us not only to describe and deepen the problem, but also to describe the analyzed information in a more coherent way, the research ends, with the conclusions and recommendations.

KEYWORDS: Crimes, Computer Data, Fundamental Law, Personal Privacy, Superior Court of Justice Puno.

INTRODUCCIÓN

En la actualidad en nuestro país, al transcurrir el tiempo se ha ido implementando leyes, con la finalidad de prevenir una de las tantas conductas ilícitas que existen, y como asi poder sancionarlas, de ello no se ha escapado los delitos informáticos que tiene como propósito afectar sistemas y las bases de datos virtuales, donde afectan los bienes jurídicos, así como el patrimonio, la libertad sexual e inclusive la fe pública.

Es cierto que con el avance de la globalización ha traído la modernización en los diferentes sistemas: tanto públicos como privados, siendo estos los que asumen identidades que no les pertenecen, realizan daños psicológicos, clonación de tarjetas bancarias, extorsionar a la población, falsificación de identidad, realizar préstamos, transferencias en entidades financieras, suplantando a las personas para recabar información secreta, sin ningún tipo de remordimiento.

La tecnología moderna con el pasar de los años va revolucionando la vida diaria de millones de personas alrededor del mundo; la informática y el internet han penetrado de una forma admirable en la vida cotidiana del ciudadano promedio en casi todos los países del mundo y, por supuesto, el Perú no es la excepción, por tal motivo esta tecnología con los sistemas de comunicación se vuelven cada vez más complejos, estas redes sociales implican que la intimidad personal pueda ser vulnerada con mucha facilidad y en diferentes formas y es por tal motivo que debe evaluarse la protección penal que se hace cuando se toca este tema en el Perú. En esta investigación no hace referencia a la información que es de carácter privado y/o reservado que de forma voluntaria se hace pública, usando las redes sociales, sino es toda información que aun teniendo carácter privado y/o reservado es totalmente transmitido de manera fraundalenta por terceros y utilizando los medios sociales.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA, ANTECEDENTES Y OBJETIVOS DE LA INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

Nuestra sociedad viene experimentando recientes formas de violación de intimidad personal así como al secreto de la comunicaciones; formas que observamos en procesos complejos de cambio creciente y apresurado que sobrepasa tanto internacionalmente como nacionalmente y de una manera muy cuidadosa también está afectando a nivel regional, en una intensidad aparentemente interminable que se caracteriza por el desafío a cada nueva norma o regulación por un nuevo elemento que trae el desarrollo de las comunicaciones y las plataformas informativas que están al alcance en nuestra vida cotidiana.

Los grandes avances tecnológicos en información y telecomunicaciones en la actualidad están logrando transformar a través de procesos experimentales y empíricos, nuevas formas de almacenamiento de información y así mismo nuevos los modos de transmisión

de la misma, que pueden llegar a ser transmisiones ilícitas que a través de sistemas informáticos estarían atentando contra los derechos fundamentales; dándose a raíz de ello la Ley de Delitos Informáticos.

El avance de las tecnologías de información y transmisión de la misma en base al llamado Internet como base e impulso para estos cambios tecnológicos que impactan en las formas de intimidad y de información que a la vez las obligan a transformarse sin proponérselo o predecirlo para poder así producir nuevas expresiones en el derecho positivo, o en las formas de determinación de la información, así como en el Derecho Penal Informático, así también provocando una reducción en los tradiciones espacios donde se desenvolvía.

Un caso emblemático internacionalmente que ocurrió fue el caso llamado “Panamá Papers” las filtraciones de los grandes casos habían tenido un componente que podría llamarse “de Estado”, es decir se recolecto, intercepto o divulgo información de índole privada en el marco de una estrategia pública. Los “Panama Papers” pusieron sobre la mesa una nueva dimensión de la misma tendencia, es decir, la actividad privada de hombres públicos y privados.

Los “Panama Papers” fue una filtración informativa de documentos confidenciales privados del estudio de abogados panameño Mossack Fonseca. Contenía 2,6 terabytes de información y fue revelado el 3 de abril del año 2016 a la vez por 109 medios de comunicación del mundo. En Perú, el portal “Ojo” Público publicó 31 entregas sobre el caso (https://panamapapers.ojopublico.com). La fiscalía peruana realiza una investigación preliminar, autorizada por el Poder Judicial hasta julio del año 2020.

Se han tornado intensos los debates que ya tenían más de un siglo, como el de la distinción de la vida privada de la intimidad personal, el secreto frente al Derecho, la

relación entre el que viola la intimidad y el que difunde esa violación, el interés público de los datos obtenidos ilegalmente y la utilidad de las pruebas obtenidas ilícitamente.

En estos procesos, el Derecho Penal se ha preocupado por desarrollar la sanción de los ilícitos más frecuentes como el uso del poder público y privado para acceder ilegalmente a datos y comunicaciones; la apropiación de códigos de acceso; y la sustracción y comercialización de bases de datos. También se ha preocupado por la protección del derecho de las personas a dar información y obtener información sobre sí mismas.

La inviolabilidad del secreto de las comunicaciones es reconocida en todos los instrumentos internacionales que garantizan los derechos humanos y se ha incorporado en nuestro ordenamiento jurídico desde la Constitución como un derecho que opera al mismo tiempo como garantía objetiva del reconocimiento de otros derechos. La existencia de una confrontación entre el secreto a las comunicaciones como derecho y la libertad de información rompe acorde a la frecuencia de las interceptaciones que se hacen a la comunicación privada para luego en un mal actuar ser disperso en los diversos medios comunicativos. En la última etapa, en el Perú, se han tenido casos que permitieron apreciar la tensión explosiva entre ambos derechos especialmente los llamados “Petroaudios”, “Potoaudios”, “Cornejoleaks”, los “Mamanivideos” y “Panama Papers”, asi también las conversaciones de por aquel entonces Juan Jiménez Mayor como premier, y el ya conocido vocal supremo César San Martin, el ministro Pedro Cateriano y la jueza Carmen Rojassi sobre la sentencia en el caso Chavin de Huantar ante la Corte IDH, llamado “Chavinaudios”, entre otros.

Lo preocupante de este problema es la interceptación de comunicaciones con fines de competencia comercial o industrial, o con propósitos de extorsión que luego son difundidos por los medios comunicativos, con ello se hace referencia al alza de vigilancia masiva de datos en el mundo dentro del cual el Perú tendría un umbral de paso con el D. L. Nº 1182, llamada también “Ley Stalker”. Estando esta como propósito de esta

investigación abordar la relación entre la ilegal interceptación y difusión de las comunicaciones y el ejercicio de las libertades informativas en el procedimiento peruano, hemos de establecer la asociación entre la característica del tipo penal y el bien jurídico protegido, dándose una estimación de su protección, así como sus restricciones y excepciones, tomando en consideración las iniciativas legislativas propuestas en los últimos años.

PROBLEMA GENERAL

¿Cómo influye el delito contra datos informáticos personales en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia Puno 2020?

PROBLEMAS ESPECÍFICOS

- ¿Cómo influye el delito contra datos informáticos personales en la dimensión de la intimidad en cuanto el derecho fundamental a la intimidad personal en la Corte Superior de Justicia Puno 2020?
- ¿Cómo influye el delito contra datos informáticos personales en la dimensión en cuanto a la privacidad en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia Puno 2020?
- ¿Cómo influye el delito contra datos informáticos personales en la dimensión en cuanto a la reserva en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia Puno 2020?

1.2 ANTECEDENTES

Al respecto Canahuire, Endara y Morante (2015) opinan que “los antecedentes son todos aquellos trabajos de investigación que preceden al que se está realizando. Son los que están relacionados con el objeto de estudio en la investigación que se está haciendo” (p. 43).

Guerra (2011) en la investigación sobre el "Derecho Penal y Derecho de las Nuevas Tecnologías de la Información y Comunicación: Criminalidad Asociada a las Telecomunicaciones", para optar el grado en Licenciatura de Ciencias Jurídicas y Sociales, en la Universidad Austral de Chile; se hace un examen a los "Delitos Informáticos" como del objeto protegido; marca: lo emitido por Brown (Uruguay), Huerta y Libano (Chile), Téllez (México), "Organización para la Cooperación y Desarrollo Económico (OCDE)" son amplios, se encuentra el contenido en valores ambiguos que se convierten en inviables, (valuación de un sistema computacional en la comisión de un ilícito). Por ello entrarían dentro de los delitos informáticos los supuestos de sustracción o daño del hardware de un ordenador. Así no se limita la conceptualización del daño producto del ilícito, y en contraposición es vaga su referencia al bien jurídico protegido en los ilícitos y si coinciden con el objeto material de tipo penal, entendiéndose de la "sana técnica informática" y daños paralelos a otros bienes jurídicos. De lo antes acotado se puede entender que estos conceptos no contribuyen doctrinariamente para precisar y definir el "Bien Jurídico Protegido" en los "Delitos Informáticos", además no se instituye con claridad los efectos de la punibilidad, dado que no se valoran y hacen referencia a los resultados del acto ilícito.

Amaya, Avalos y Jule (2012), en la investigación sobre el "*Derecho a la Intimidad en la estructura de la ley especial de intervención de telecomunicaciones*" para optar el grado de Licenciatura de Ciencias Jurídicas en la Universidad de El Salvador, acerca de la relación existente de las Telecomunicaciones y el "Derecho a la Intimidad", se concluye que la existencia de factores que limitan dichos derechos como son: la seguridad del Estado, bienestar general, el desorden, el crimen y la protección a la Salud; asimismo, establece que la intervención entre ambas figuras jurídicas, está marcada por la posible vulneración al "Derecho a la Intimidad" cuando estas son realizadas en forma ilegítima; por otro lado señala que la intervención a las telecomunicaciones limita al derecho de la intimidad y su protección, requiriendo este derecho la tutela por parte del órgano Estatal para lograr el fin

de una convivencia en paz acorde a una sociedad que se dirija a ello en concordancia con este derecho personalísimo y que además se encuentra protegido por instrumentos internacionales. También es de señalar que no todos los países cuentan con normatividad específica a telecomunicaciones y siendo las leyes existentes en casos excepcionales; respecto a la jurisprudencia como fuente desde el derecho, a guiar las decisiones y esclarecer el procedimiento a llevarse a cabo en el análisis de la injerencia en los derechos de intimidad de las personas, con la finalidad de no colisionar con otros derechos.

Del mismo modo, Zaballos (2013) en la investigación sobre "*La protección de datos personales en España: Evolución normativa y criterios de aplicación*" para optar el grado de Doctor en Derecho, de Universidad Complutense de Madrid – España, se concluye: a las causantes económicas, sociales y tecnológicas que colaboran al aumento de riesgo en la normatividad que tenga relación a la "protección de datos personales" sean preventivas, opinando que con la finalidad de minimizar el avance delictivo en temas relacionados con la tecnológica e informática, se hace viable realizar cambios de materia, medios e instrumentos que permitan el desarrollo del conocimiento y este la productividad y competitividad en equilibrio con los "derechos y libertades de los individuos". Así mismo la protección de los datos personales se contempla dentro de las telecomunicaciones, de la seguridad y de la administración pública y servicios sanitarios entre otros; este contexto de datos personales entra en la obligatoriedad de los países de la revisión y análisis de su ordenamiento jurídico. La configuración de principios generales de datos personales, consentimiento, finalidad, información y tratamiento se debe de respetar y adecuarse a los mismos, derivando una serie de obligaciones administrativas, civiles y penales en caso de incumplimiento; también, se debe tener especial consideración el principio de confidencialidad, como el llamado deber de secreto, cuál es la protección de los datos personales privados, cautelando todo poder y control de los mismos de esta forma se obliga a los responsable del tratamiento de esta información a crear medios que aseguren el cumplimiento de estos, junto al cumplimiento de sistema de seguridad cuál condición

primordial en la legitimidad de la protección de datos que incumban a organizaciones privadas y públicas cuya función incluya procedimientos con datos y sistemas de información personal, así su finalidad entra dentro de la protección de los datos cuya incidencia que pudiera provocar su destrucción, alteración o intromisión no autorizada.

Alarcón Ariza, Diego Alexander, Barrera Barón, Javier Antonio “Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica” Universidad Privada Norbert Wiener, Escuela de Posgrado, Lima, 2017. CONCLUSIÓN: La red digital trae consigo oportunidades y peligros, estos plantean desafíos tanto políticos como éticos. Lograr introducir valores éticos y moralidad social a los nuevos avances en información es en sí mismo el fin y contribución a la sociedad y su desarrollo. Las instituciones universitarias han de cumplir un rol formador y de responsabilidad social en el fomento de normatividad acorde y en línea a estas problemáticas y regulaciones referentes a derechos de autor. Cada institución debe tener claramente formulados unos compromisos éticos que le permitan definir con claridad el papel que juega la institución y 9 de cada uno de 46 sus miembros, de esta red de información en una contextualización de pluralidad, igualdad, respeto, honradez, justicia, libertad y solidaridad. Desde el plano internacional la Organización de Cooperación y Desarrollo Económico (OCDE) de 1983, da inició al estudio de posibilitar la aplicación y armonización de leyes en el plano internacional en perspectiva penal que luchen contra la utilización de programas computacionales usados de forma ilícita. En 1992, la OCDE elabora una conjunción normativa para la seguridad de la información con base en que los Estados en conjunto con el sector privado den un contexto claro de seguridad para sistemas de información. Dentro de los alcances que debemos prescindir en la sociedad es mantener un comportamiento ético, honesto y denunciar las actividades fraudulentas y delictivas de cualquier integrante de la comunidad Universitaria.

Sequeiros Calderón, Ivett Claritza "*Vacíos legales que imposibilitan la sanción de los delitos informáticos en el nuevo Código Penal Peruano-2015*", Universidad De Huánuco Facultad De Derecho Y Ciencias Políticas, Huánuco, 2016. Resumen: el desarrollo y evolución de la tecnología informática en una forma delictual dentro de la criminalidad de los delitos informáticos y en este contexto el Perú ha dado normatividad para prevenir y sancionar estas conductas de gran afectación a sistemas de información y de telecomunicaciones, así como a los demás bienes jurídicos tutelados que puedan ser afectados como la libertad sexual, la fe pública y el patrimonio. La Ley N° 30096 "Ley de delitos informáticos" fue promulgada el 21 y publicada el 22 de octubre del 2013 en el diario oficial "El Peruano". Luego fue parcialmente modificada por la Ley N° 30171 "Ley que modifica la Ley 30096, Ley de delitos informáticos", promulgada el y publicada el de marzo del 2014. No se ha de desconocer los beneficios y utilidad de los sistema informáticos a causa de algunas conductas ilícitas, los beneficios de esta tecnología es evidente, asi como el mal uso e intento de mal uso por entes y personas en contra de la sociedad dentro de los cuales se encuentran delitos como la pesca de los datos "pishing", la penetración en redes informáticas, la piratería digital, el envío de correo basura, la propagación maliciosa de virus y otros ataques contra las infraestructuras de información esenciales.

Espinoza Vilchez, July Soledad "El derecho a la intimidad y su protección en el sistema jurídico peruano" Universidad Nacional Mayor de San Marcos, Facultad de Derecho y Ciencia Política-Unidad de Posgrado, Lima 2018. Resumen: se asume desde un enfoque de regulación y aplicabilidad en el ordenamiento jurídico del derecho de intimidad. El derecho en mención es uno de los que acarrean más vulneración directa e indirecta por la sociedad y los medios de la prensa, programas televisivos, archivos informáticos, redes sociales, entre otros. Este derecho ha tenido protección y defensa a niveles culturales y de formas en que la sociedad concibe la dignidad y la libertad de la información, y a pesar de la existencia de normatividad y regulación constitucional al respecto no han sido de todo

efectividad y no han estado acorde a los cambios acelerados. Se da un predominio de la desinformación en la aplicación y la posible publicidad de agravio en contra de los afectados, así como la falta de protección por las sentencias que en casos de enfrentamiento a derechos de información y libertad de expresión, dentro de la hipótesis se ha demostrado que factores legales, procesales y sociales han de cumplir un papel importante en la valoración y defensa de este derecho.

Romilio Quintanilla Chacón (2010), en su tesis de investigación "Publicaciones de los medios de prensa escritos regionales y los delitos contra el honor de las personas en la región de Puno, año 2010", cuyos objetivos de determinar las causales por las cuales no se denuncian penalmente los informes periodísticos que atenten al honor de las personas (p. 4); por lo cual se usó el la metodología analítica de diseño no experimental; en cuyas conclusiones de "La desconfianza en la administración de justicia (PJ, MP y PNP) y el desconocimiento de la normatividad en relación a ilícitos contra el honor, y con ello son también causas del porque los agraviados no denuncian estos los ilícitos a pesar de sentir vulnerado su honorabilidad. Los irrisorios montos de reparación civil y la improbabilidad de su ejecución es también un factor que desanima a los agraviados a denunciar estos delitos". (p. 157)

María Cecilia Rojas Guanilo (2015), en su tesis "Las nuevas formas de materialización de la libertad de expresión y la vulneración del derecho a la intimidad de la persona", busca en sus objetivos, establecer de qué manera en nuestro país las nuevas formas de manifestación de la Libertad de expresión como el internet, Facebook, Twitter, WhatsApp, hangouts, entre otros, así también programas de corte periodístico o pseudo periodístico, ponen en vulnerabilidad al derecho a la intimidad, en el momento en que presentan situaciones de conflictos entre éstos (p. 10), y concluye: "No existen medios eficaces para la adecuada regulación, supervisión y fiscalización de la información privada e íntima que

es divulgada en los medios de comunicación, y particularmente la que es difundida por la red de internet mediante Facebook, Twitter, WhatsApp, hangouts, entre otros y la contenida en programas de corte periodístico o pseudo periodístico, encontrándonos en un entorno que vulnera el derecho a la intimidad (como libertad fundamental del ser humano) al no contar con una tutela y cautela que determine y sancione de manera efectiva al transgresor". Todas las personas sin distinción ni justificación alguna gozan de una "legítima expectativa" de protección y respeto de su vida privada e intimidad por lo que el público no tiene un legítimo interés de conocer su paradero o cómo actúa en su vida privada, no obstante, se encuentre en lugares públicos o que sea conocido públicamente". (p. 145)

Vega Aguilar J. A. (2010) con la tesis de título "Los delitos informáticos en el Código Penal" por la Universidad católica de Santa María, con el fin de optar el grado académico de Maestro en Derecho Penal; el autor del trabajo mencionado, pudo concretar las siguientes conclusiones relacionadas a nuestro tema: El avance científico y tecnológico han acarreado aspectos positivos e importantes de la sociedad de nuestro tiempo, motivando el desfase de la interpretación tradicionalista de los tipos penales producto del avance de estos ilícitos de avance y evolución constante de nueva data como es la criminalidad informática. La ausencia de una nomenclatura clara inexistente actualmente que abarque toda la problemática referida a la criminalidad informática hace que a nuestra posición la llamemos "Criminalidad informática", debido a la novedad de uso conductual de los ilícitos como nueva forma de criminalidad. Que, estos delitos de nueva data son delitos pluriofensivos, debido a que afectan a más de un bien jurídico protegido, con son el patrimonio, el honor, la intimidad, el pudor, el orden económico, la libertad informática, la vida el cuerpo entre otros, que afectan en agravio de la sociedad y del desenvolvimiento de la misma. Así es un desatino la inclusión de los Delito informáticos dentro del Capítulo del título de los delitos contra el patrimonio en el código penal que permite colegir que solo

existen Delitos informáticos Contra el Patrimonio, de todas partes incongruente con la realidad, dada la gama de constante evolución de nuevas formas de criminalidad en afectación de bienes jurídicos como el patrimonio, el honor, la intimidad, el pudor, la libertad informática, la vida el cuerpo y la salud, etc. El entorno de virtualidad de estas formas de criminalidad entran en confusión de la tipificación y de la realización de investigación de la PNP; asimismo en la actualidad los magistrado del poder judicial y del ministerio público tiene poca experiencia en las áreas de Derecho informático cuya fin esboza el enfrentar la nueva forma de criminalidad. Finalmente se puede apreciar la escasa investigación en procesos penales en relación con los delitos informáticos, los mismos que se encuentran tipificados en nuestro Código Penal vigente en los artículos 2O7o "A",2O7o "B'y 2O7o "C" los cuales fueron incorporados en nuestro Código Penal vigente mediante Ley No 27309 "Ley que incorpora los Delitos informáticos en el Código Penal" de fecha 17 de julio del 2000, motivando la posible derogatoria de los artículos antes mencionados y realice una análisis pormenorizado de los tipos penales que pueden ser realizados por medios informáticos del Código Penal vigente, los cuales deben ser agravados debido al impacto que ocasiona en nuestra sociedad.

1.3 OBJETIVOS DE LA INVESTIGACIÓN

OBJETIVO GENERAL

Determinar la influencia del delito contra los datos informáticos personales en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno 2020.

OBJETIVOS ESPECÍFICOS

- Determinar la influencia del delito contra los datos informáticos personales en la dimensión intimidad del derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno 2020.
- Determinar la influencia del delito contra los datos informáticos personales en la

dimensión privacidad del derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno 2020.

- Determinar la influencia del delito contra los datos informáticos personales en la dimensión de reserva del derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno 2020.

1.4 JUSTIFICACIÓN

No se encuentra en discusión el planteamiento del problema sobre el derecho a la intimidad personal en sí mismo y en su componente del secreto de las comunicaciones, siendo obvio que el Derecho Penal se esfuerza por actualizar la protección de estos bienes jurídicos cuya vigencia es presionada por el desarrollo de las tecnologías de la información de uso privado, individual y corporativo, y por políticas desarrolladas desde los mismos estados jurídicos, lo que se ha visto hoy en dia un alto grado de vulnerabilidad de las personas sintiéndose inseguras y desprotegidas por nuestro estado.

En esta última época, en el Perú, se han registrado casos que han permitido evaluar esa tensión y, al mismo tiempo, la dificultad de resolver la relación conflictiva entre derechos y libertades, con resultados no siempre relacionados tanto en la vía penal como en la constitucional. El tema de esta investigación es actualmente poco tratado por el Estado peruano y los agentes judiciales, la facilidad en que se perpetua el delito de la violación a la intimidad personal y la violación a los datos informáticos personales hoy en día se está empezando a dar con más frecuencia también por redes sociales y lo más vulnerable que somos hoy en día a afectaciones mediante las redes sociales a nuestra buena imagen, nuestro honor, en razón de que al día millones de personas interactúa mediante alguna red social, sin tener conocimiento de si, verdaderamente muchas de estas cuentas son de personas reales o son creadas por mentes delictivas y con ansias de encontrar nuevas víctimas, no solamente en delitos de violación a la intimidad existen, millones de delitos que se dieron a causa de las redes sociales.

En la última etapa, en el Perú, se han registrado casos que han permitido apreciar esa tensión y, al mismo tiempo la dificultad de resolver la relación conflictiva entre derechos y libertades, con resultados no siempre coherentes tanto en la vía penal como constitucional, por esa razón, la investigación se propone relevar y profundizar en el interés público para superar esa tensión, de modo que ninguno de los derechos y libertades en juego en este caso deje de cumplir su papel de protección jurídica considerando como muy necesario que se optimice el derecho de la sociedad a estar informada de los asuntos públicos.

1.5 HIPÓTESIS

1.5.1 HIPÓTESIS GENERAL

- El delito contra datos informáticos personales influye significativamente en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020.

1.5.2 HIPÓTESIS ESPECÍFICAS

- El delito contra datos informáticos personales influye significativamente en la dimensión intimidad en cuanto al derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020.
- El delito contra datos informáticos personales influye significativamente en la dimensión en cuanto a la privacidad del derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020.
- El delito contra datos informáticos personales influye significativamente en la dimensión en cuanto a la reserva en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020.

CAPÍTULO II

MARCO TEÓRICO, CONCEPTUAL E HIPÓTESIS DE LA INVESTIGACIÓN

2.1. MARCO TEÓRICO

DELITO INFORMÁTICO.

Dar un marco definitorio de los delitos informáticos no es tarea sencilla, dada la no existencia de consensos a nivel doctrinario ni jurisprudencial en términos del Derecho Penal, en parte al constante cambio y evolución en esta actividad delincuencial en materia informática se encuentra comprendida dentro de una serie de acciones que es difícil de reducir o agrupar en una sola definición.

Villavicencio (2014), entiende como: “aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología” (p. 286).

Del mismo modo el Dr. Acurio (2012) profesor de Derecho Informático de la PUCE, sobre la definición y concepto de “Delitos Informáticos” señala:

> […] que Delincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como objetivo poner en peligro o dañar cualquier bien jurídico. (p. 14)

Además, el Dr. Blossiers (2003) indica que:

> Cuando hablamos de Delitos Informáticos estamos hablando sobre delitos instrumentales mediante el uso del computador. . . . De igual forma precisa que "la criminalidad informática exige una legislación penal especial, al darse ésta podría integrarse una amplia gama de conductas delictivas, que a pesar de que actualmente se han incorporado en nuestra ley penal sustantiva, aún resulta muy limitada y necesita ineludiblemente enriquecerse. (pp. 137-152)

De igual modo, el profesor Sáez (2002) expresa "en general, para gran parte de la doctrina no existe un delito informático, sino una realidad criminal compleja vinculada a las nuevas técnicas de información, imposibles de ser incluidas en un único tipo legal" (p. 21).

Por otro lado, Reyna (2002) indica:

> Que si bien existen diferencias claras entre ambos conceptos - delitos computacionales y Delitos Informáticos - ambos forman parte de un mismo fenómeno criminal cuya denominación correcta sería la de criminalidad mediante computadoras y por la cual debe de entenderse a todas las conductas criminales para cuya comisión se emplee los ordenadores o en las cuales resulte afectada la información contenida en los sistemas informáticos. (p. 139)

Fernández Villegas, Vivanco Quinto y Vara Morocco (2018) El Delito informático, es el derecho y la sociedad siempre están en constante cambio, por lo que es el derecho quien ha de adecuarse a las necesidades. Se puede señalar que los principales cambios se han dado por el progreso o la constante actualización tecnológica informática inmersa en gran parte de los aspectos de la vida en sociedad. Así surge comportamientos ilícitos que se

denominan genéricamente como delitos informáticos donde los sujetos activos en actos dolosos afectan a otro sujeto pasivo dañando y vulnerando su privacidad, intimidad, y el patrimonio. En esta oportunidad abordaremos el tema de los Delitos informáticos, y para ello es necesario saber que la informática se refiere al procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales, que cuentan y están capacitados para cubrir básicamente tres tareas: entrada (captación de la información), procesamiento y salida (transmisión de los resultados). Así a las mencionadas se les conoce como algoritmo.

El Instituto de Tecnologías Educativas de España (ITE), vivimos en un mundo globalizado donde el uso de ordenadores y programas informáticos permiten el acopio, ordenación, procesamiento y aplicación de información en usos diversos que permitan un célere progreso tecnológico, aun así ello ha conseguido la dependencia tecnológica de la sociedad, que abarca fabricantes de distintos rubros de equipos y de los mismos programas informáticos, también de quienes aprovecha un cierto conocimiento del tema para acceder al hogares, centros de trabajo, empresas y en todo lugar donde la delincuencia pueda obtener algún tipo de beneficio, sin duda los usos de la informática se ha extendido a procesos industriales, comerciales y financiero, sino también ha tenido una incidencia más alta en el uso de las redes sociales, así el Instituto de Tecnologías Educativas de España (ITE) indica que el uso de las redes sociales en nuestros jóvenes es una realidad que depende de nosotros como sociedad que el uso de esa tecnología sea usada para su bien (ITE, párr. 2), de lo anteriormente señalado podemos advertir que son dos los factores que impulsan al legislador a tomar la decisión de legislar a favor de una ley propia donde se dé la regulación del uso de la informática por los, en relación también a la integridad e indemnidad sexual, entendido de esta forma se expresan factores base para que conlleven al legislador a impulsar la promulgación de la Ley de Delitos Informáticos, ley N° 30096 en adelante (LDI), fueron dos bienes jurídicos principales: i) Uno fue la indemnidad sexual de los menores, y ii) El perjuicio patrimonial de las personas y

empresas, ello a través de la vulneración del patrimonio que se resguarda la integridad de los programas informático ello al ser considerado bienes de gran importancia, es así que la industria del software viene en un creciente dinamismo.

CEPAL (2009) indica que en América Latina ha ocurrido de forma esencialmente espontánea, considerando que hace muy poco tiempo se pusieron en marcha políticas públicas de estímulo al sector (p. 1). y iii) el tercer bien jurídico que la ley busque proteger es el de la privacidad, entendida en su generalidad, pues abarca la privacidad nuestras comunicaciones, de nuestros documentos, archivos de familia, etc.

Navarro (s.f.) expresa del derecho a la intimidad está basado en el pacto social, que dicta el respeto de todas las personas entre sí, así se refiere al que marco los límites de este derecho donde abogados de Norteamericana de Boston los doctores Samuel D. Warren y Louis Brandeis que denominaron a este derecho “right of privacy” derecho que conocemos como derecho a la privacidad, otro bien jurídico protegido el programa en cuanto a su integridad y funcionamiento, situación que motiva al legislador a tipificar el atentado o el daño al sistema como un ilícito penal.

En síntesis, advertimos que los bienes jurídicos que se sustentan para los delitos informáticos serán:

1.- La indemnidad o integridad sexual de los menores, este bien jurídico se vulnera cuando sujetos contactan con menores ocultando su identidad e intenciones, iniciando una supuesta amistad que conlleva a propuestas que atentan la integridad sexual del menor, chantaje, proposiciones sexuales, violaciones, etc.

2.- El perjuicio patrimonial de las personas naturales y empresas, en estos casos se tiene la sustracción de dinero de cuentas bancarias, estafas,

3.- La privacidad de comunicaciones, de documentos, de registros y la privacidad del entorno familiar, todo ello engloba la privacidad propiamente dicha, el entorno familiar implica privacidad personal y familiar, siendo privacidad género e intimidad especie.

El uso de la informática tiene diversos usos en algunos casos sirven como medios de comunicación Messenger, Correo Electrónico, Facebook, Twitter, WhatsApp, Instagram entre otros, en otros casos sirven para el procesamiento de información como office, Linux, etc., el avance de la informática y su aplicación a casi todos los ámbitos de la actividad humana ha traído como resultado que se crea una dependencia en la tecnología y a la vez se dé una oportunidad para el aprovechamiento por parte de personas que actúan al margen de la ley y buscan el aprovechamiento de estas oportunidades, ello puede verse en las sustracciones de cuentas vía internet, la clonación de tarjetas, etc. El legislador en cumplimiento de su deber de legislar, pero con poca técnica ha incorporado en un cuerpo normativo las conductas punibles relacionadas a la informática que en un inicio se 24 encontraba tipificado en el Art. 186° inc. 3, segundo párrafo del Código Penal de 1991; posterior se legisla y lo ubicamos en la Ley Nº 30096 “Ley de Delitos Informáticos”; que fuera modificada por la ley N° 30171 que introdujo modificaciones a la ley antes señalada.

Código Penal Peruano Delitos informáticos

Nuestra normatividad del Código Penal en el artículo 207-A, hace la definición del delito informático en cuanto al que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

Tenemos como ejemplo que se desprende de esta premisa, aquellos fraudes que se cometieron en perjuicio de las instituciones bancarias o de cualquier empresa por personal

del área de sistemas que tienen acceso a los tipos de registros y programas utilizados. También se encuadra el fraude efectuado por manipulación informática, es decir, cuando se accede a los programas establecidos en un sistema de información y se les manipula para obtener una ganancia monetaria. (Fernández Villegas, Vivanco Quinto, & Vara Morocco, 2018)

Tenemos también a la falsificación informática, la misma que se configura con la operación de aquellos datos que específicamente son confidenciales por la importancia que tienen, como la repetición de programas que ameritan ser guardados bajo seguridad absoluta, por el derecho que tienen sus propios autores, acreditada como piratería, Así mismo, su artículo 207-B., hace referencia a la alteración, daño, y destrucción de datos, sistema de red o programa de computadoras, donde se señala que:

> Aquel que maneja, integra, ilegalmente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días de multa. (Código Penal, art. 207-B)

En este caso, podemos señalar que este artículo hace referencia al manejo o al hecho de integrar de manera ilícita determinados datos que más adelante serán dañados o de alguna manera tratar de beneficiarse con aquella información obtenida, utilizándolos para un fin que perjudica a terceras personas.

Se puede señalar que existe, la Ley 27309, la misma que añade los delitos informáticos al Código Penal en el que específicamente solo se ha señalado dos aspectos en general, los mismos que cuentan con diversas características. Por lo mismo es que el legislador, tiene como fundamento primordial, el uso de la computadora como herramienta para cometer los delitos informáticos.

> Esta Ley de delitos informáticos, establece especialmente penas para atentados contra la integridad de datos informáticos, sistemas informáticos, proposiciones a niños y adolescentes con fines sexuales, incitación a la discriminación, contra la

> intimidad y el secreto de las comunicaciones como el tráfico ilegal de datos, la interceptación de datos informáticos, suplantación de identidad, abuso de mecanismos y dispositivos informáticos y el fraude informático. El aumento de la criminalidad informática en el Perú y a nivel mundial trae consigo consecuencias económicas y numerosos fraudes cometidos por organizaciones delictivas que muchas veces no son denunciados o cuyos delitos son cometidos en el exterior sin que muchas veces exista una sanción. (Dávila Laguna, 2017)

Estructura general del "delito contra datos y sistemas informáticos"

Sujeto activo. En los delitos contra datos y sistemas informáticos el sujeto activo es cualquier persona humana capaz que tenga conocimiento de tecnología informática.

Sujeto pasivo. Asimismo, en estos delitos el sujeto pasivo de la acción son los datos y sistemas informáticos; del mismo modo el sujeto pasivo del delito es la información, entendiéndose como información al conjunto de datos contenidos en sistemas informáticos cuyo titular es la persona natural o jurídica.

Bien Jurídico Protegido. En el "delitos contra datos y sistemas informáticos" se puede advertir que la información al ser almacenada, tratada y transmitida eficientemente genera una ventaja ante el resto de la sociedad.

Al respecto Reyna (2001) señala que "el bien jurídico penal a tutelar sería la información como valor económico de empresa, el mismo que no solo constituye un interés social vital, sino que cumple con las exigencias de merecimiento de protección y necesidad de tutela,... " (p. 252).

Comportamiento delictivo. De la propia norma, ley 30096 se puede advertir que el comportamiento delictivo consiste en un primer momento solo y únicamente cuando se ingresa a un sistema informático sin autorización; transgrediendo así los sistemas de protección para ello; o excediendo lo autorizado.

Por otro lado, en un segundo momento el accionar delictivo consiste en “introducir, borrar, deteriorar, alterar, suprimir o hacer inaccesible los datos informáticos a través de las Tecnologías de la Información o Comunicación.”

Asimismo, en un tercer momento el acto ilícito consiste en inutilizar un Sistema Informático total o en parte impidiendo el acceso, entorpeciendo o imposibilitando la prestación de sus servicios para su eficiente funcionamiento de las “Tecnologías de la Información o Comunicación”.

Confidencialidad de sistema informático. Se puede mencionar que la confidencialidad es sumamente importante por lo que se debe de tener en cuenta que, con la finalidad de proteger los datos informáticos, este solo deberá de ser conocida por personas que se encuentren facultadas, una de las formas de atentar contra la privacidad se da en la comunicación de información. (Bradanovic, 2006, párr. 20).

Derechos Humanos y Derechos Fundamentales. Se entiende como derechos humanos a las demandas derivadas básicamente de la dignidad de la persona, derechos se encuentran dentro de la esfera de ética diferente a la esfera del derecho positivo. Motivo por el cual los derechos humanos se encuentran fuera de la Constitución, pero sirven de fundamento axiológico para los derechos fundamentales; en tanto una Constitución vigente y concreta no reconozca a los derechos humanos, estos no convierten en derecho fundamentales, perdurado en el tiempo solo como demandas, por lo tanto, no pueden ser exigidas y tuteladas jurídicamente. Sin embargo dado un análisis constitucional de los cuerpos de las cartas magnas actuales y vigentes, en estas se incluye una relación extensa de derechos incluso más amplia que la “Declaración Universal de Derechos Humanos”, clasificándose como excepción.

INTIMIDAD PERSONAL:

El derecho a la intimidad se encuentra reconocido en tratados e instrumentos internacionales y en esa medida ha alcanzado un estándar similar al de otros derechos considerados esenciales, como el derecho a la vida y a la libertad y seguridad personal. La Declaración Universal de Derechos Humanos (1948) consigna en su artículo 12° una visión que garantiza la intimidad desde la perspectiva de impedir injerencias más que invasiones arbitrarias:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. (art. 12)

Del mismo modo, la Convención Americana sobre Derechos Humanos (1969) reconoce el derecho a la intimidad en el artículo 11°, en el sentido clásico que relaciona la dignidad y la honra:

> Protección de la honra y de la dignidad
>
> 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
> 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
> 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. (art. 11)

La Corte IDH ha calificado este concepto como no susceptible de definiciones exhaustivas precisando que no se refiere exclusivamente a la protección de la honra o de la reputación sino también al derecho a la vida privada y la intimidad (CORTE IDH, Sentencia Serie N.° 215 párrafo 129, 2010). Coincidentemente, la versión en inglés de este artículo se titula *Right to privacy* y no protección de la honra y de la dignidad.

El Pacto Internacional de los Derechos Civiles y Políticos (1966) preconiza esta visión, aun cuando incorpora en su texto además de lo señalado, un ámbito de intimidad relacionado a la vida privada y al derecho a no ser molestado. El artículo 17° señala lo siguiente:

> 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
>
> 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. (art. 17)

Existen también diferentes normas internacionales de los últimos años que progresan el principio aplicándolo a actividades detalladas. Es el caso de la Convención sobre los Derechos del Niño (1989) cuyo artículo 16° se traduce como protección de las disposiciones de los tratados internacionales, del modo siguiente:

> Tienen derecho a una vida privada propia, a que se respete la vida privada de su familia y a la intimidad de su domicilio; a que no abran su correspondencia y a que nadie ataque su imagen. (art. 16)

Al respecto, el Tribunal Constitucional del Perú (STCNº 6712-2005-HC/TC, F. J.38), respecto al "Derecho Fundamental a la Intimidad" señala que la esfera no conocida o difundida de una persona es la vida privada, y por lo tanto nadie puede tener acceso a ella sin su consentimiento; por otro lado dentro del derecho positivo se puede establecer que es el espacio personal en el cual el sujeto se encuentra facultado para desarrollar e impulsar en forma libre su personalidad; entonces se puede afirmar que está formada por información, hechos o circunstancias ignorados por la sociedad, reservándose solo y únicamente a su persona o un grupo reducido; cuya trasgresión genera un perjuicio.

Derecho a la Intimidad Personal

Fayos et al. (2015) señala que el derecho a la intimidad tiene como función principal "proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida

personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad" (p. 66).

Carbonell (2006) establece que existen dos formas de atentar contra la intimidad de las personas; en un primer momento a través de la invasión de un espacio personal, llamado también "intimidad territorial"; y en un segundo momento a través del conocimiento de cualquier forma sobre circunstancias, datos o información relacionada a la vida privada del individuo, llamado también "intimidad informacional" (p. 2).

Scalvini y Leyva (2002) afirman que:

> "El derecho a la intimidad" avala al titular a desarrollarse libremente dentro de su espacio privado, sin perturbación alguna de terceras personas o de las autoridades, entendiéndose que dicha conducta desarrollada no contravenga al orden público y que no perjudique el derecho de las personas. (p. 2038)

Con respecto a este punto Meján (1994) sostiene lo siguiente:

> Es un Derecho Fundamental que asiste a los sujetos de derecho consistente en la facultad de mantener en reserva sobre diversas situaciones relacionadas con la vida privada, que debe ser reconocido y regulado por el sistema jurídico y que es oponible a todos los demás salvo en los casos en que puede ser develado por existir un derecho superior de terceros o para el bienestar común. (p. 69)

Por lo tanto, se puede decir que es el derecho atribuido a toda persona de mantener un espacio secreto o reservado para los asuntos vinculados a su vida particular; y que dichos datos, hechos o situaciones son desconocidos por la sociedad, estando por lo tanto son reservados al conocimiento solo y únicamente del titular del derecho, o reducidos estos a un grupo de personas; sin participación de individuo alguno; derecho conocido también como "el libre desarrollo de la personalidad".

En tal sentido, la información protegida bajo este ámbito son los siguientes:

- Datos personales relacionados a la "intimidad personal y familiar"
- Salud personal

- Comunicaciones, telecomunicaciones y documentos privados en general.

- Los denominados datos sensibles.

El derecho a la intimidad en nuestro sistema jurídico peruano

Al tenerse presente el contexto de la persona en general existe la necesidad de proteger su intimidad desde el ámbito jurídico, tomando como base la intimidad como fuente de creatividad, de ideas y opiniones personales, y es el impulso para el ejercicio de los demás derechos, resultando ser la expresión máxima del derecho a la libertad y la posibilidad de un desarrollo armonioso de la persona en la colectividad y además siguiendo posiciones doctrinarias, el Perú comienza a reconocer y proteger la intimidad como tal, recién la constitución 1979 en el inc. 5 del Art. 2.

Vale decir que, mientras que en Estados Unidos se posiciona el inicio de la autonomía del derecho a la intimidad en 1890, en el Perú las normas relativas a este derecho se hacen presente en la constitución de 1979.

Es en dicho documento constitucional ya derogado que aparece por primera vez reconocido el derecho a la intimidad personal y familiar en nuestro sistema jurídico. En ese entender, con la promulgación del Código Civil de 1984, al regularlo más específicamente, el legislador nacional le dio real presencia y contenido en nuestro sistema jurídico. En efecto el Art. 14 del citado código, expone la no exhibición de la intimidad de la vida familiar y personal sin el consentimiento de las personas, o en el caso del fallecimiento con el consentimiento de sus conyugues o descendientes o ascendientes u hermanos respetando ese orden.

Sin embargo, en la práctica resultaba evidente que las normas civiles por si solas, eran de escasa efectividad, pues la vulneración de la intimidad personal seguía su curso inexorable en perjuicio de la personalidad de su titular, haciéndose uso para ello de instrumentos, procesos técnicos o medios electrónicos. En tal sentido, el legislador del Código Penal de 1991, siguiendo las tendencias modernas del derecho punitivo, no le quedó otra alternativa

que incorporar el derecho a la intimidad cual bien jurídico penal, así interés factible de protección penal, cuanto su desprotección lesionaría de forma grave las relaciones interpersonales en la sociedad. Así, aparecen, varias conductas delictivas en las cuales la intimidad es el bien jurídico protegido. Este acontecimiento se presenta como toda una innovación en nuestro derecho penal.

En efecto, en nuestro Código Penal encontramos el título IV con el rótulo de delitos contra la libertad y en ese rubro, el Capítulo II con el nomen iuris de la violación de la intimidad, donde aparecen diversas conductas delictivas, como son: "*vulnerara la intimidad de la vida personal o familiar del agraviado, ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios parecidos*"; apareciendo como circunstancia agravante el hecho de revelar lo conocido indebidamente y tener al sujeto activo como calidad de funcionario o servidor público. Otro hecho punible lo constituye el revelar aspectos de la intimidad personal o familiar del agraviado, que conociera el sujeto activo

con motivo del trabajo que presto a su víctima o a la persona que lo confió, y finalmente, se ha tipificado como hecho punible cuando el agente indebidamente organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o varias personas, apareciendo como agravante la calidad del sujeto activo de funcionario o servidor público, siempre que haya actuado dolosamente en el ejercicio del cargo que desempeña. Bramon Arias Torres sostiene que el criterio principal que ha llevado a regular esas conductas en el código penal es el avance tecnológico alcanzado en nuestra sociedad, el que hace posible que se realice conductas dirigidas a afectar la intimidad o a controlar a las personas. (Arias Torres, 1994)

2.2 MARCO CONCEPTUAL

INFORMÁTICA Y DATOS PERSONALES

DEFINICIÓN DE DERECHO INFORMÁTICO

Julio Téllez (s.f.) define al derecho informático como: “el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática”.

Por otra parte Delpiazzo (s.f.) nos dice que pueden distinguirse en ese término, dos acepciones: “el Derecho Informático como una rama del Derecho integrada por las normas y principios que se refieren a la actividad informática y por otro, una ciencia que tiene por objeto el estudio del sector jurídico”.

Por lo que, podemos definir como derecho informático, al conjunto de normas jurídicas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones, tiene por objeto la información.

INFORMÁTICA E INTIMIDAD

Los beneficios que trae la tecnología de información, presenta a su vez riesgos y peligros a la intimidad como.

Gilberto Alcala (s.f) establece cuatro categorías:

a) una invasión a la zona de privacidad,

b) la difusión de hechos privados embarazosos,

c) una publicidad que coloque a la persona en falsas posiciones ante los ojos de los ciudadanos y

d) indebida apropiación del nombre o apariencia de una persona.

Por otro lado, el avance de la tecnología ha hecho posible la existencia eficiente de bancos de datos, antes existían pero sus alcances eran limitados; en uno de los aspectos más específicos, alude a las centrales de riesgo crediticio, desde que nació la informática y el almacenaje y procesamiento de datos, comenzó la preocupación sobre su uso.

Algunas legislaciones se ocuparon y llegaron a la distinción en lo que se denominaron datos sensibles de una persona, la posibilidad de registrar un sin fin de datos personales, permite reconstruir hasta los detalles más recónditos de la vida.

Linch afirma que un ciudadano estadounidense genera diariamente 150 registros digitales; si se repara en que éstos almacenan tales contactos y todos ellos podrían concentrarse en una base de datos, a partir de allí es factible conocer hasta los detalles más recónditos de la vida de la persona; siempre han existido datos aunque no en la cantidad y calidad que ahora y la posibilidad teórica de reunirlos.

Pero la informática ha permitido el salto potencial de acceder casi de inmediato a todos esos datos, clasificarlos, ordenados, permite también formular programas de interpretación de tales datos; a partir de allí la vida del usuario queda expuesta.

Aproximadamente en los años '60 la atención se centró en el uso de la información personal y se fue expandiendo contemporáneamente con la proliferación de las computadoras. En los últimos años se ha producido una espiral de utilización de información personal que se consolida con la difusión de internet; esto significa el acceso de millones de personas, que hoy se estiman en más de 50 millones, en un mismo espacio virtual y así se multiplican las posibilidades de invasión a la intimidad en el Internet.

La utilización exponencial de medios digitales multiplica obviamente la información almacenada y las bases de datos; por lo que genera una nueva masa de información personal expuesta al público; en el tiempo en que estas bases de datos no eran cuantiosas o cuando su generación era deliberada el control sobre las mismas era más factible cuando. La Internet agrega elementos delusorios de la intimidad: es que si tendrá tanta incidencia en la vida de las personas, y bajos índices de seguridad, la vida de la persona quedará más expuesta que antes.

El uso básico de preferencias de una persona queda establecidas en la red, brindando información utilizable y de interés, así está la información sobre consultas médicas,

permitiendo a través de estudios elaborar perfiles ideológicos, sanitarios o intelectuales de cada persona, el desafío es mejorar la seguridad de la utilización de los datos personales.

Los estudios sobre la interferencia de la informática en la intimidad no son nuevos, pues ya tienen más de dos décadas; sin embargo, el ingreso en la Era Digital provoco una explosión del problema, el principal medio Internet y una sus funciones como el correo electrónico tiene serios problemas de seguridad en la protección de datos personales en nuestro país.

En tanto comienzan a intercambiar datos más de 50 millones de usuarios dispersos en el mundo, proliferan los mercados electrónicos, las publicaciones en línea, los requerimientos de información, los requerimientos de servicios, la actividad del teletrabajo, las interconsultas médicas, las videoconferencia, los mensajes personales enviados y recibidos, abre un amplio campo de riesgo para la intimidad.

Es necesario una mayor protección de la intimidad, un agravamiento y ampliación de las figuras protectoras, mayores exigencias de seguridad para quienes almacenan los datos personales.

DELITOS INFORMÁTICOS Y DATOS PERSONALES

La conjunción entre el avance acelerado de la tecnología de información y su influencia en la sociedad actual, que abarca gran parte del comportamiento social de interacción entre las personas, ha traído consigo estas formas de ilícitos que denominamos en general, delitos informáticos.

El autor mexicano Julio Tellez Valdez señala que los delitos informáticos “son actitudes ilícitas en que tienen a las computadoras como instrumento o fin, son conductas antijurídicas y culpables ".

Rafael Fernández Calvo define al delito Informático como “cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito Informático, es cualquier acto

ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

Por lo que podemos definir qué, los delitos informáticos, son cualquier comportamiento criminal en que la computadora está involucrada como material u objeto; es toda acción u omisión culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima.

La informática está hoy presente en casi todos los campos de la vida moderna; con mayor o menor rapidez todas las ramas del saber humano se generan ante los progresos tecnológicos, ejecutando así un gran número de tareas que en otros tiempos serían ejecutadas de forma manual y personal. El progreso cada día más importante y sostenido de los sistemas de computación, permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de usuarios.

José Luis Castillo (s.f.) nos dice que:

> Las perspectivas de la informática no tienen límites previsibles y aumentan en forma vertiginosa. Las facilidades que pone a los usuarios, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario que nuestra legislación regule los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

TIPOS DE DELITOS INFORMÁTICOS

Podemos clasificarlos de la siguiente forma:

a) Como instrumento o medio, se tienen a las conductas criminales, que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.

b) Como fin u objetivo, en ésta categoría se enmarcan las conductas criminales van dirigidas en contra de la computadora, accesorios o programas como entidad física.

DELINCUENTE INFORMÁTICO

Para Julio Téllez (s.f.) el “delincuente informático es la persona o grupo de personas que en forma asociada realizan actividades ilegales haciendo uso de las computadoras y en agravio de terceros, en forma local o a través de Internet”.

Así tenemos como uno de las formas delictuales más numerosas el interceptar la información de las compras en línea para la información personal interceptada como el nombre, número de tarjeta de crédito y fecha de expiración, se realizan compras diversas de cualquier bien, entre software, hardware, y a las cuales para la entrega de los bienes se colocan direcciones para dejar el producto distintas a la utilizadas por el titular en la tarjeta. Es también un delincuente informático el "pirata" que distribuye software sin contar con las licencias de uso proporcionadas por su autor o representantes, pues no solo atenta contra la propiedad intelectual, que provoca la fuga de talentos en informática, a su vez está enriqueciéndose ilegalmente y está siendo un evasor de impuestos.

2.3 HIPÓTESIS DE LA INVESTIGACIÓN

HIPÓTESIS GENERAL

El delito contra datos informáticos personales influye significativamente en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020.

HIPÓTESIS ESPECÍFICOS

- El delito contra datos informáticos personales influye significativamente en la dimensión intimidad en cuanto al derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020.
- El delito contra datos informáticos personales influye significativamente en la dimensión en cuanto a la privacidad del derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020.
- El delito contra datos informáticos personales influye significativamente en la

dimensión en cuanto a la reserva en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. ZONA DE ESTUDIO

La presente investigación será realizada en la Corte Superior de Justicia de Puno durante el periodo 2020. Dicha institución se encuentra en el departamento de Puno, provincia y distrito de Puno.

3.2 TAMAÑO DE MUESTRA

Se tomará como población a los profesionales del derecho que trabajan en la “Corte Superior de Justicia de Puno”, periodo 2020.

Está constituida específicamente por los profesionales del derecho que trabajan en la Corte Superior de Justicia de Puno, que conocen la materia, y es de tipo probabilístico porque al ser escogidos al azar cada uno de las unidades de análisis de la población tienen la misma posibilidad; obteniéndose en base a las particularidades de la población; se utilizará el método probabilístico para establecer la dimensión de la muestra; por otro lado, la selección de los elementos de análisis fue en forma aleatoriamente.

3.3 MÉTODOS Y TÉCNICAS

MÉTODOS

La presente investigación adopta el método hipotético – deductivo, comparativo y sintético - analítico, esto con la finalidad de obtener conocimiento, a continuación, expondremos cada uno de ellos. El método hipotético – deductivo, que implica la contrastación de hipótesis a través de la deducción, tenderá a la verificación de las hipótesis ya planteadas de la influencia de los “delitos contra datos informáticos personales” en las dimensiones intimidad, privacidad y reserva del “derecho fundamental a la intimidad personal”, esto a partir de los datos recogidos.

En el método sintético–analítico se pasará analizar cada una de las variables (delito contra datos informáticos personales y el derecho fundamental a la intimidad personal) en forma independiente, para así poder pronunciarse sobre todo el conjunto, con la finalidad de producir un conocimiento.

Y por último en el método comparativo lo que se va buscar es la comparación de la variable independiente delito contra datos informáticos personales y con la variable dependiente el derecho fundamental a la intimidad personal.

TÉCNICA

Como técnica se utilizará la encuesta, la misma que tiene como propósito encontrar la información que se requiere, de la unidad de análisis, basado en hechos, opiniones, conocimientos, actitudes o sugerencias y el instrumento que se elaborará será el cuestionario de preguntas.

Instrumento de investigación

Además, los instrumentos a utilizarse en la presente investigación fueron:

Fichas bibliográficas. Instrumentos que sirven para tomar anotaciones de documentos bibliográficos y de toda fuente de información correspondiente al “derecho fundamental a la intimidad personal” y el “delito contra los datos informáticos”.

Cuestionarios. Son instrumentos que contienen las preguntas de carácter cerrado del “delito contra los datos informáticos personales” así como del “derecho fundamental a la intimidad personal”. Una de las peculiaridades principales que tiene este tipo de instrumento es que sus preguntas son cerradas con un cuadro de respuestas respectivamente; esto es en virtud del poco tiempo que tienen los encuestados para responder.

Guías de análisis documental. Este instrumento es utilizado como una guía en el acopio de información a obtener relacionado al “derecho fundamental a la intimidad personal” y el “delito contra los datos informáticos personales”.

La técnica para la recolección de datos se ejecutó con la encuesta y el instrumento que se utilizó fue el cuestionario por 15 ítems aplicado a los trabajadores de la Corte Superior de Justicia, la consistencia de la fiabilidad del instrumento es a través del coeficiente de Alpha de Cronbach para instrumentos politómicos conforme a la escala de likert.

Tabla 1

Estadísticas de fiabilidad del instrumento de recolección de datos

Alfa de Cronbach	N de elementos
,905	25

Fuente: Elaboración Propia

Verificando la tabla de resultados se obtuvo que de la recolección de datos con 25 ítems una confiabilidad de Alpha de Cronbach un equivalente al 0,0905 (90,5%), lo que se muestra una confiabilidad del instrumento muy alta para hacer su aplicación.

3.4 IDENTIFICACIÓN DE VARIABLES

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR	ITEMS	INSTRUMENTO
El delito contra datos informáticos personales	"Conducta típica, antijurídica y reprochable en las cuales se utilizan a las computadoras como instrumento" *(Núñez 1996. p. 251-252).*	Es la variable que mide el acto ilícito mediante el cual se transgrede la confidencialidad de datos y de sistemas informáticos personales.	- Confidencialidad de información personal. - Integridad de sistemas informáticos	- Acceso deliberado - Acceso ilegítimo - Vulneración de seguridad - Inutiliza - Impedir acceso - Entorpecer su funcionamiento	1 y 2 3 y 4 5 y 6 7 8 9	Cuestionario sobre los delitos contra datos informáticos personales.
El derecho fundamental a la intimidad personal	Es el derecho subjetivo reconocido a favor de una persona, con la	Variable que mide la intromisión de aquella esfera íntima, privada y	- Intimidad	- Personal - Dignidad - Espiritual	1 y 2 3 y 4 5	Cuestionario sobre el derecho

	finalidad de proteger su esfera individual de la intromisión de extraños *(Celis 2006. p. 74)*	reservada que tiene toda persona, la misma que se encuentra protegida por el Derecho.	- Privacidad --- - Reserva	- Prácticas sexuales. - Condiciones de salud. - Comunicaciones personales --- - Información - Propiedad - Libertad de conciencia	6 y 7 8 9 y 10 --- 11, 12 y 13 14 15 y 16	fundamental a la intimidad personal

3.5 MÉTODO O DISEÑO ESTADÍSTICO

La investigación fue de enfoque cuantitativo, de tipo básico en razón de crear conocimiento y teorías a partir del fenómeno investigado, se utilizó la técnica de las encuestas (el muestreo, por cuanto se va a elegir 25 elementos al azar y en forma aleatoria de una población de 200 profesionales del derecho de la Corte Superior de Justicia de Puno), con el instrumento de fichas bibliográficas, cuestionarios y guías de análisis documental.

CAPÍTULO IV

EXPOSICION Y ANALISIS DE RESULTADOS

En esta parte se presentan los resultados de la aplicación del instrumento de recolección de datos a una muestra de 200 trabajadores de la Corte Superior de Justicia de Puno.

En la variable independiente, delito contra los datos informáticos personales, de un total de 90 puntos como el máximo que pudiera obtener cada encuestado en el cuestionario sobre el delito contra los datos informáticos personales, los 200 profesionales del derecho de la muestra hicieron una media de 83.0545 +/- 1.97165 y en el promedio, los puntajes se alejan de la media de 3.887 unidades (tabla 3).

En cada una de las dos dimensiones de esta variable se obtiene como máximo 30 puntos, la más alta en la dimensión confidencialidad de información personal (27.89 +/- 1.208), esto quiere decir que la confidencialidad de información personal afecta casi de la misma forma como la integridad de sistemas informáticos.

Tabla 2

Medidas estadísticas de la variable “delito contra datos informáticos personales” y sus dimensiones.

Variable/Dimensiones	Media	Desv. Tip.	Varianza
Delito contra datos informaticos personales	83.0545	1.97165	3.887
Confidencialidad de informacion personal	27.89	1.208	1.459
Integridad de sistemas informáticos	27.6864	1.32306	1.750

Fuente: cuestionario

La variable el delito contra datos informáticos personales mide la influencia de la confidencialidad de información personal, integridad de sistemas informáticos en el derecho fundamental a la intimidad personal, la figura 1 nos muestra que el delito contra datos informáticos realizada por estos es en el nivel medio (100%).

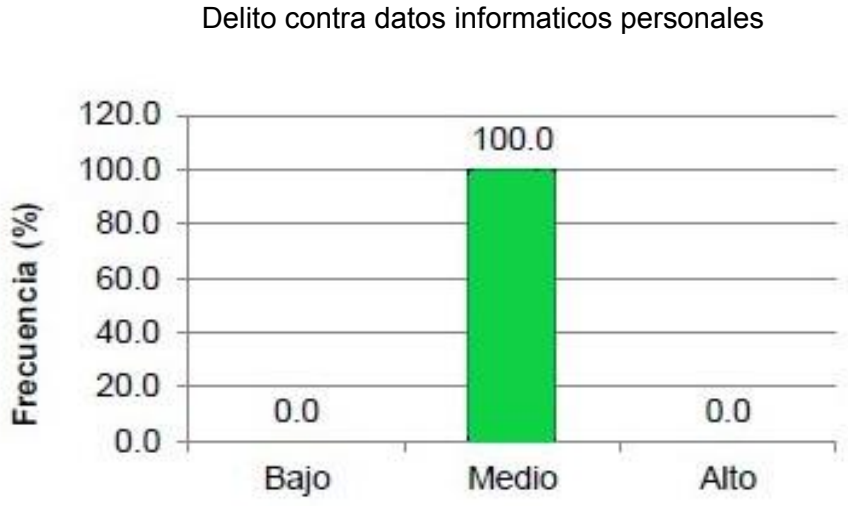

Figura 1. Frecuencia porcentual de la variable delito contra datos informáticos personales

Delito contra datos informáticos personales en la modalidad de confidencialidad de información personal, una de las modalidades de los delitos contra datos informáticos personales es la confidencialidad de sistemas informáticos, viendo la opinión de los operadores del derecho de la Corte Superior de Justicia de Puno, esta influencia está en el nivel medio (100%) figura 2

Figura 2. Frecuencia porcentual del delito contra datos informáticos personales en la modalidad de confidencialidad de información personal realizada por los operadores del derecho de la Corte Superior de Justicia de Puno.

Delito contra datos informáticos personales en la modalidad de integridad de sistemas informáticos, es otra de las modalidades de los delitos contra datos informáticos personales es la integridad de sistemas informáticos en opinión de los operadores del derecho de la Corte Superior de Justicia de Puno, esta influencia está en el nivel medio (100 %) figura 3.

Integridad de sistemas informáticos

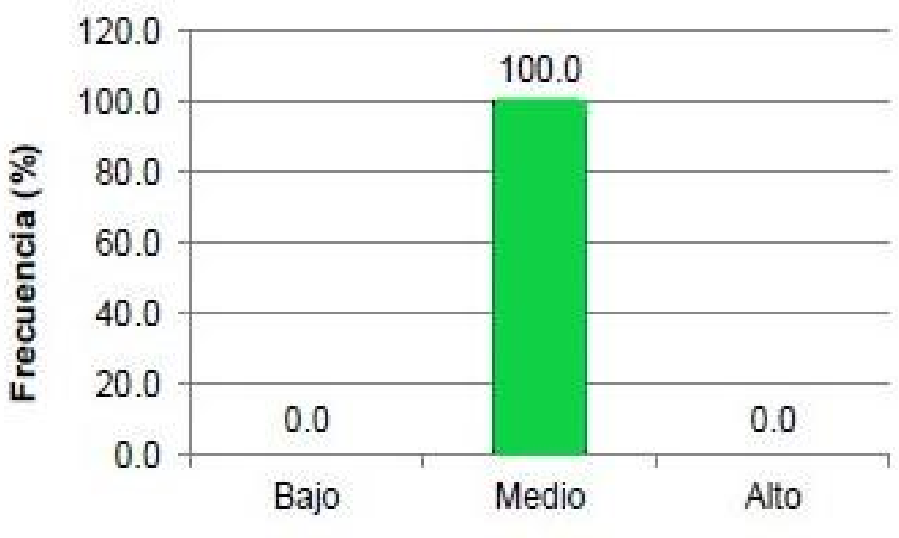

Figura 3. Frecuencia porcentual del delito contra datos informáticos personales en la modalidad de integridad de sistemas informáticos por los operadores del derecho de la Corte Superior de Justicia de Puno.

La variable dependiente, derecho fundamental a la intimidad personal, asimismo, con el cuestionario respecto al derecho fundamental a la intimidad personal, se obtiene 90 puntos como máximo y 30 puntos como mínimo se puede obtener de cada encuestado, los 200 profesionales del derecho de la muestra hicieron una media de 81.5682 +/- 1.45241 en promedio los puntajes se alejan de la media en 2.109 unidades de la tabla 4. La variable el derecho fundamental a la intimidad personal se ve que es menor al de los delitos contra datos informáticos personales. De la misma manera en cada una de las tres dimensiones de esta variable se obtiene como máximo 30 puntos, la dimensión más baja que se pudo observar es en la dimensión reserva 27.0727 +/- 1.13241 y la mas alta que se pudo observar es la dimensión intimidad 27.3636 +/- 1.11222. El derecho fundamental a la intimidad personal y cada una de las dimensiones son regulares para los operadores del derecho de la Corte Superior de Justicia de Puno.

Tabla 3

Medidas estadísticas de la variable derecho fundamental a la intimidad personal y sus respectivas dimensiones.

Variable/Dimensiones	Media	Desv. Tip.	Varianza
Derecho fundamental a la intimidad personal	81.5682	1.45241	2.109
Intimidad	27.3636	1.11222	1.237
Privacidad	27.1318	1.22228	1.493
Reserva	27.0727	1.13241	1.282

Fuente: cuestionario

La mediación de la variable en el derecho fundamental a la intimidad personal, tomamos en cuenta la intimidad, privacidad y la reserva, según como podemos apreciar en la figura 4 de los operadores del derecho de la Corte Superior de Justicia de Puno, se evidencia un nivel medio de afectación a este derecho (100%).

Figura 4. Frecuencia porcentual del derecho fundamental a la intimidad personal

En la intimidad la opinión de los operadores del derecho de la Corte Superior de Justicia de Puno, revelan que se afecta en un nivel medio (100%) figura 5.

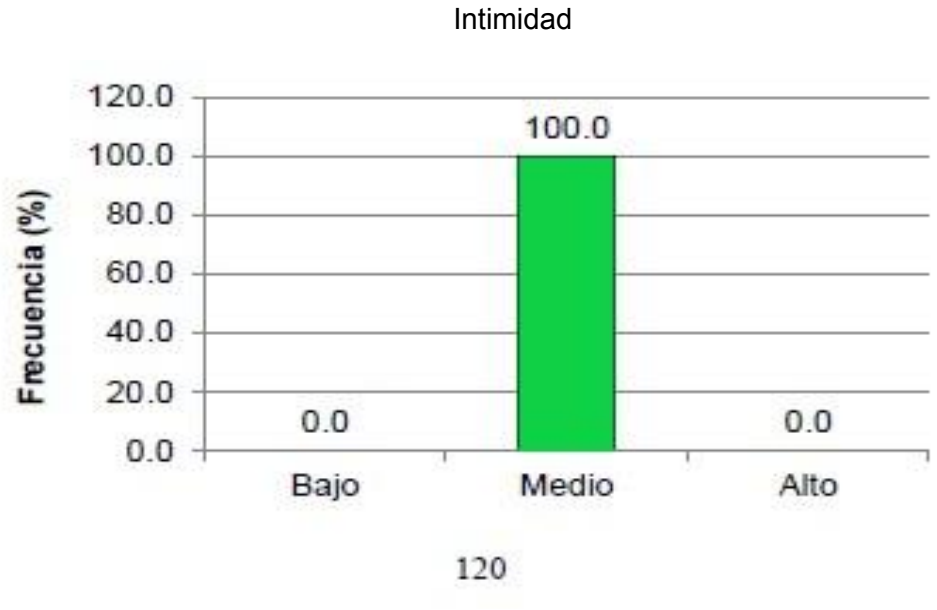

Figura 5. Frecuencia porcentual de la intimidad realizada por los operadores del derecho de la Corte Superior de Justicia de Puno.

En la privacidad los operadores del derecho de la Corte Superior de Justicia de Puno, opinan que se afecta este derecho en un nivel medio (100%) figura 6.

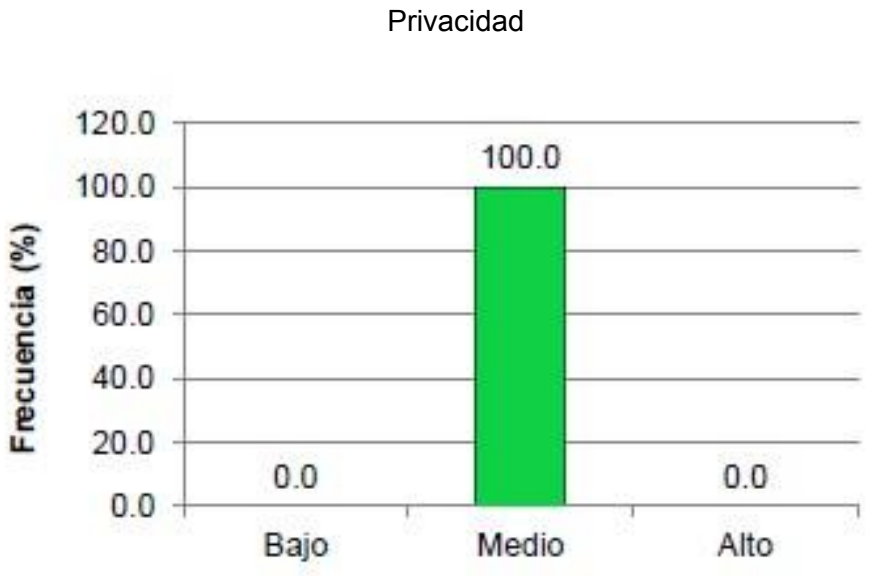

Figura 6. Frecuencia porcentual de la privacidad realizada por los operadores del derecho de la Corte Superior de Justicia de Puno.

En la reserva los operadores del derecho de la Corte Superior de Justicia de Puno analizaron que la reserva como parte integrativa del derecho fundamental a la intimidad personal afecta un nivel medio (100%) figura 7.

Figura 7. Frecuencia porcentual de la reserva realizada por los operadores del derecho de la Corte Superior de Justicia de Puno.

CONCLUSIONES

PRIMERO. Se pudo determinar que en criterio de los operadores del derecho de la Corte Superior de Justicia de Puno, los delitos contra datos informáticos personales han demostrado tener un impacto significativo en el derecho fundamental a la intimidad personal. Existe una correlación positiva promedio significativa entre las variables involucradas (delito contra datos informáticos personales y en el derecho fundamental a la intimidad personal). Los delitos contra datos informáticos personales en las modalidades de confidencialidad de información personal e integridad del sistema informático afectan al 28% de los "derecho fundamental a la intimidad personal".

SEGUNDA. Se pudo determinar que en criterio de los operadores del derecho de la Corte Superior de Justicia de Puno, los delitos contra datos informáticos personales han demostrado tener un impacto significativo en la intimidad del derecho fundamental a la intimidad personal. Existe una correlación positiva muy débil pero significativa entre la variable delitos contra datos informáticos personales y con la dimensión intimidad, el delitos contra datos informáticos personales afectan la intimidad del derecho fundamental a la intimidad personal en un 18%.

TERCERO. Se pudo determinar que en criterio de los operadores del derecho de la Corte Superior de Justicia de Puno, los delitos contra datos informáticos personales han demostrado tener un impacto significativo en la privacidad del derecho fundamental a la

intimidad personal. Existe un vínculo positivo pero importante entre la variable delito contra datos informáticos personales y la dimensión privacidad. Los delitos contra datos informáticos personales afectan al 57% de la privacidad del derecho fundamental a la intimidad personal.

CUARTO. Se pudo determinar que en criterio de los operadores del derecho de la Corte Superior de Justicia de Puno, los delitos contra datos informáticos personales han demostrado tener un impacto significativo en la reserva del derecho fundamentales a la intimidad personal. Existe una correlación positiva débil pero significativa entre la variable delito contra datos informáticos personales y la dimensión reserva, el delito contra datos informáticos personales afectan el 86% a la reserva del derecho fundamental a la intimidad personal.

RECOMENDACIONES

PRIMERO. Es oportuno señalar a través del Poder Judicial que el Estado continúe capacitando a los legisladores de la Corte Superior de Justicia de Puno, sobre los principios generales de protección de la información pública y privada (información confidencial, manejo). Restricciones a la información personal, verdades actualizadas, seguridad personal, indemnización civil para garantizar que los derechos fundamentales de la privacidad personal y familiar estén protegidos de actividades ilícitas cometidas con la ayuda de computadoras.

SEGUNDO. Es importante recordar que la intimidad es un derecho constitucional y siempre debe protegerse de la actividad ilegal, especialmente los delitos contra los datos y los sistemas informáticos. Este crimen viola implícitamente el honor y la dignidad de una persona. Por lo tanto, los profesionales del derecho deben ser conscientes de que la clasificación de actividad ilegal realizada por las computadoras se inspira en la protección de la información personal y familiar y afecta la privacidad personal.

TERCERO. También se debe enfatizar que el derecho a ser notificado debe combinarse con los derechos de todos los seres humanos para proteger la privacidad de los datos. Por lo tanto, los abogados deben ser conscientes de que obtener información con fines

de lucro u otros fines no puede violar la dignidad y la moral de las personas. Para proteger su privacidad.

CUARTO. Como principio de promoción, el principio y la condición son excepciones. Los operadores de la ley están obligados a evaluar las reservas de documentos que contienen información personal con base en los principios básicos y la protección de valores que promueven su confidencialidad; por otro lado, son donde vivimos. Otros derechos fundamentales (defensa y acceso a la justicia) deben estar comprometidos, al igual que los relacionados con la sociedad en la que viven.

BIBLIOGRAFÍA

Aira, H., M. (2008). El criterio de Bien Jurídico Penal que adopta el Tribunal Constitucional. Lima: Pontificia Universidad Católica del Perú. Recuperado de: http://blog.pucp.edu.pe/item/26299/el-criterio-de-bien-JURÍDICO-penal-que-adopta-el-tribunal- constitucional

Agüero, A. (2007). El Comercio Electrónico, Los "Delitos Informáticos" y su Legislación en Venezuela (2001-2006). Para optar el Titulo de Magister Scientiae en Administración. Universidad de los Andes. Venezuela.

Alexy, R. (2007). Teoría de los Derechos Fundamentales. Madrid: revista Cuestiones Constitucionales. Nº 17.

Alvarado, T., K. (2015). El libre desarrollo de la personalidad. Análisis comparativo de su reconocimiento constitucional en Alemania y España. Perú. Revista de Investigación Jurídica. Nº 10.

Amaya, T., Avalos, A. y Jule F. (2012). Derecho a la Intimidad en la estructura de la ley especial de intervención de telecomunicaciones. Para optar el grado de Licenciado en Ciencias Jurídicas. Universidad de El Salvador, San Salvador.

Arata, Á., A. (2002). Tesis: Las nuevas Tecnologías de la Información y la Problemática Jurídica del Comercio Electrónico. Para optar el Título Profesional de Abogado. Universidad Nacional Mayor de San Marcos. Perú.

Balmaceda, Q., J. (2008). Revista de investigación Jurídica. Recuperado de: www.usat.edu.pe/usat/.../BIEN-JURÍDICO-JUSTO-BALMACEDA1.

Blossiers, H., J. (2003). Criminalidad Informática. Lima: Edit. Librería Portocarrero.

Blossiers, M., J., y CALDERON, G., S. (2000). Delitos Informáticos en la Banca. Lima, Perú: Editora RAO SRL.

Bradanovic, P., T. (2006). Conceptos básicos de seguridad informática. Chile

Bramont – Arias, T., L. (1997). El Delito Informático en el Código Penal Peruano. Lima, Perú. Fondo Editorial de la Pontificia Universidad Católica del Perú.

Camacho, Cano, Neira, Ovalle y Villamil (2013). La información reservada en el ordenamiento jurídico colombiano. Colombia. Revista de Derecho Penal y Criminología. Volumen XXXVI. Nº 96.

Canahuire, A. Endara, F. y Morante, E. (2015). ¿Cómo hacer la tesis universitaria? Una guía para investigadores. Cuzco: Colorgraf.

Carbonell S., M. (2005), Teoría constitucional y derechos fundamentales. (2da. Ed.). México: Porrúa.

Fayos, G., A. y otros (2015). Los derechos a la intimidad y a la privacidad en el siglo XXI. Madrid, España. Editorial Dykinson, SL. Meléndez Valdés.

Fernández, T. (2012). Diseño del trabajo de investigación. Trujillo: Universidad Cesar Vallejo.

Ferro V., J. (2016). Seguridad Informática: Aspectos Generales y Especiales. España: Autoediciones Tagus

Hernández, M., A. (2004). Tesis: Los Delitos a través del uso de la Computadora. México. Para obtener el Título de Abogado. Presentada en la Universidad Autónoma de San Luis de Potosí. Bolivia.

Hernández, R., Fernández, C., Baptista, M. (2014). Metodología de la Investigación. Sexta Edición. México. Interamericana Editores S.A de C.V.

Instituto Nacional de Estadística e Informática (INEI.). (2000). Amenazas en Internet. Lima, Perú. Editorial Oficina Técnica de Administración del INEI.

Instituto Nacional de Estadística e Informática (INEI.). (2000). Conceptos sobre seguridad de la información. Lima, Perú. Editorial Oficina Técnica de Administración del INEI.

Instituto Nacional de Estadística e Informática (INEI.). (2001). Delitos Informáticos. Lima, Perú. Editorial Oficina Técnica de Administración del INEI.

Mejan C., L. (1994). El Derecho a la Intimidad y la Informática. (1ra. Ed.). México: Porrúa.

Méndez, J., F. (2009). Tesis: “Delitos Informáticos”. Para obtener el Título de Licenciado en Derecho. Presentada en la Universidad Michoacana de San Nicolás de Hidalgo. México.

Ministerio Público (2017). Boletín estadístico del Ministerio Público. Recuperado de: http://www.mpfn.gob.pe.

Palacios, D. y Mongue, R. (2003). Las Constituciones del Perú 1823 - 1993. Lima, Perú. Editora FECAT.

Poder judicial (2017). Cuadro de asignación de personal. Recuperado de: https://www.pj.gob.pe. Res.

Poder Judicial del Perú. Acuerdo plenario Nº 03-2006-CJ/116. Delitos contra el honor personal y derecho constitucional al derecho de expresión y de información. Recuperado de: https://www.pj.gob.pe/wps/wcm/connect/1e3604004075bad5b75ff799ab657107/acuerdo_plenario_03-2006_CJ_116.pdf?MOD=AJPERES&CACHEID=1e3604004075bad5b75ff799ab657107

Reátegui, J. (2009). Derecho Penal – Parte General. Lima, Perú. Gaceta Jurídica S. A.

Reyna, L., M. (abril 2001). El bien jurídico en el delito informático. Lima: revista electrónica de derecho informático, Alfa – Redi, Nro. 33.

Reyna, L., M. (2002). Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal. Lima – Perú. Juristas Editores.

Riascos, L. (1999) Tesis: El "Derecho a la Intimidad", la visión iusinformatica y el delito de los datos personales. Para optar el Título de Doctor en Derecho. Presentada en la Universidad de Lleida, España. España.

Sáenz, C., J. (2002). "Delitos Informáticos" o Delitos Cometidos por medios informáticos. Argentina. Revista de Derecho Informático Alfa – Redi, Nro. 45.

Sánchez, M., A. (2014). El alcance del "Derecho a la Intimidad" en la sociedad actual. España. Revista de Filosofía.Org.

Tribunal Constitucional del Perú (2005). STC 1417-2005-PA/TC. Caso Manuel Anicama Hernandez. Recuperado de: https://tc.gob.pe/jurisprudencia/2005/01417-2005-AA.pdf

Villa, E., J. (2014). Derecho Penal Parte General. Lima – Perú. ARA Editores E.I.R.L.

Villavicencio, T., F. (2014). "Delitos Informáticos". Perú. Revista IUS VERITAS, Nro. 49.

Vives, T., S. & ORTS, E. (2010). Derecho Penal Parte Especial. 3ra. Edición. Valencia – España. Tirant lo Blanch.

Warre, S. y Brandeisei, L. (1995) "Derecho a la Intimidad". Madrid. Civitas, 1995.

Zaballos, E. (2013) Tesis: La "protección de datos" personales en España: Evolución normativa y criterios de aplicación. Para optar el Título de Doctor en Derecho. Presentada en la Universidad Complutense de Madrid. Madrid, España.

ANEXOS

ANEXO 1

[“Ley Nº 30096 - Ley de Delitos Informáticos”]

LEY DE DELITOS INFORMÁTICOS

LEY Nº 30096

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

CAPÍTULO I

FINALIDAD Y OBJETO DE LA LEY

Artículo 1.- Objeto de la Ley

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

CAPÍTULO II

DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS

Artículo 2.- Acceso ilícito

El que 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 modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"Artículo 2. Acceso ilícito

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

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

Artículo 3.- Atentado 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. (*)

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"Artículo 3.- Atentado a la integridad de datos informáticos

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

Artículo 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. (*)

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"Artículo 4. Atentado a la integridad de sistemas informáticos

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

CAPÍTULO III

DELITOS INFORMÁTICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES

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

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

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

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

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

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

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

CAPÍTULO IV

DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Artículo 6.- Tráfico ilegal de datos

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

(*) Artículo derogado por la Única Disposición Complementaria Derogatoria de la Ley N° 30171, publicada el 10 marzo 2014.

Artículo 7.- Interceptación de datos informáticos

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

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

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

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"Artículo 7- Interceptación de datos informáticos

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

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

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

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

CAPÍTULO V

DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 8. Fraude informático

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

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

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"Artículo 8. Fraude informático

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

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

CAPÍTULO VI

DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

Artículo 9.-Suplantación de identidad

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

CAPÍTULO VII

DISPOSICIONES COMUNES

Artículo 10.- Abuso de mecanismos y dispositivos informáticos

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

(*) Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, especificamente 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.

"Artículo 12.- Exención de responsabilidad penal

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

(*) Artículo incorporado por el Artículo 3 de la Ley N° 30171, publicada el 10 marzo 2014.

DISPOSICIONES COMPLEMENTARIAS FINALES

PRIMERA.- Codificación de la pornografía infantil

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

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

SEGUNDA.- Agente encubierto en delitos informáticos

El fiscal, atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa mediante tecnologías de la información o de la comunicación, con prescindencia de si los mismos están vinculados a una organización criminal, de

conformidad con el artículo 341 del Código Procesal Penal, aprobado mediante el Decreto Legislativo 957.

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

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

(*) Disposición modificada por el Artículo 2 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

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

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

CUARTA.- Cooperación operativa

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

(*) Disposición modificada por el Artículo 2 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

"CUARTA. Cooperación operativa

Con el objeto de garantizar el intercambio de información, los equipos de investigación conjuntos, la transmisión de documentos, la interceptación de

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

QUINTA.- Capacitación

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

SEXTA.- Medidas de seguridad

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

SÉTIMA.- Buenas prácticas

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

OCTAVA.- Convenios multilaterales

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

NOVENA.- Terminología

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

a. Por sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus

elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

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

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

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

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

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

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

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

(*) Disposición modificada por el Artículo 2 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente:

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

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

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

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

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

DISPOSICIONES COMPLEMENTARIAS MODIFICATORIAS

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

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

"Artículo 1. Marco y finalidad

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

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

1. Secuestro.
2. Trata de personas.
3. Pornografía infantil.
4. Robo agravado.
5. Extorsión.
6. Tráfico ilícito de drogas.

7. Tráfico ilícito de migrantes.

8. Delitos contra la humanidad.

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

10. Peculado.

11. Corrupción de funcionarios.

12. Terrorismo.

13. Delitos tributarios y aduaneros.

14. Lavado de activos.

15. Delitos informáticos."

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

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

"**Artículo 3.- Delitos comprendidos**

La presente Ley es aplicable a los siguientes delitos:

(...)

9. Delitos informáticos previstos en la ley penal."

TERCERA. -Modificación del Código Procesal Penal

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

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

(...)

4. Los concesionarios de servicios públicos de telecomunicaciones deberán facilitar, en el plazo máximo de treinta días hábiles, la geolocalización de teléfonos móviles y la diligencia de intervención, grabación o registro de las

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

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

(*) Confrontar con el Artículo 6 de la Ley N° 30171, publicada el 10 marzo 2014.

Artículo 235. Levantamiento del secreto bancario

(...)

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

Artículo 473.- Ámbito del proceso y competencia

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

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

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

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

"Artículo 162.- Interferencia telefónica

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

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

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

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

(*) Confrontar con el Artículo 4 de la Ley N° 30171, publicada el 10 marzo 2014.

Artículo 183-A.- Pornografía infantil

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

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

1. El menor tenga menos de catorce años de edad.
2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del artículo 173 o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será

no menor de doce ni mayor de quince años. De ser el caso, el agente será inhabilitado conforme a los numerales 1, 2 y 4 del artículo 36.

Artículo 323.- Discriminación

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

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

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

(*) Confrontar con el Artículo 4 de la Ley N° 30171, publicada el 10 marzo 2014.

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

ÚNICA. Derogatoria

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

Comuníquese al señor Presidente Constitucional de la República para su promulgación.

En Lima, a los veintisiete días del mes de setiembre de dos mil trece.

FREDY OTÁROLA PEÑARANDA

Presidente del Congreso de la República

MARÍA DEL CARMEN OMONTE DURAND

Primera Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

POR TANTO:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiún días del mes de octubre del año dos mil trece.

OLLANTA HUMALA TASSO

Presidente Constitucional de la República

JUAN F. JIMÉNEZ MAYOR

Presidente del Consejo de Ministros

ANEXO 2

MATRIZ DE CONSISTENCIA

TÍTULO: EL DELITO CONTRA DATOS INFORMÁTICOS PERSONALES EN EL DERECHO FUNDAMENTAL A LA INTIMIDAD PERSONAL EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO, 2020.

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES
GENERAL: ¿Cómo influye el delito contra datos informáticos personales en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia Puno 2020?	**GENERAL:** Determinar la influencia del delito contra los datos informáticos personales en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno 2020.	**GENERAL:** El delito contra datos informáticos personales influye significativamente en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020.	**INDEPENDIENTE:** Delito contra datos informáticos personales.	- Confidencialidad de informacion personal - Integridad de sistemas informáticos	- Acceso ilegítimo - Vulneración de seguridad - Impedir el acceso -Imposibilitar su funcionamiento -Entorpecer su funcionamiento
ESPECÍFICOS: ¿Cómo influye el delito contra datos informáticos personales en la dimensión de la intimidad en cuanto al derecho fundamental a	**ESPECÍFICOS:** Determinar la influencia del delito contra los datos informáticos personales en la dimensión intimidad del derecho	**ESPECÍFICOS:** El delito contra datos informáticos personales influye significativamente en la dimensión intimidad en cuanto al derecho	**DEPENDIENTE:** Derecho fundamental a la intimidad personal.	- Intimidad	- Dignidad - Cultural - Personalísimo - Espiritual

la intimidad personal en la Corte Superior de Justicia Puno 2020? ¿Cómo influye el delito contra datos informáticos personales en la dimensión en cuanto a la privacidad en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia Puno 2020? ¿Cómo influye el delito contra datos informáticos personales en la dimensión en cuanto a la reserva en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia Puno 2020?	fundamental a la intimidad personal en la Corte Superior de Justicia de Puno 2020. Determinar la influencia del delito contra los datos informáticos personales en la dimensión privacidad del derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno 2020. Determinar la influencia del delito contra los datos informáticos personales en la dimensión de reserva del derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno 2020.	fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020. El delito contra datos informáticos personales influye significativamente en la dimensión en cuanto a la privacidad del derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020. El delito contra datos informáticos personales influye significativamente en la dimensión en cuanto a la reserva en el derecho fundamental a la intimidad personal en la Corte Superior de Justicia de Puno, 2020.		- Privacidad - Reserva	- Comunicaciones personales - Condiciones de salud - Creencias religiosas - Prácticas sexuales - Libertad de conciencia -Información - Propiedad

ANEXO 3

Matriz de recolección datos

Especificaciones del cuestionario sobre los delitos contra datos informáticos personales

Variable/Dimensiones		Indicador	Item	Puntaje Mínimo	Puntaje Máximo
Delito contra datos informaticos personales	Confidencialidad de informacion personal	- Acceso deliberado - Acceso ilegítimo - Vulneración de seguridad	1 y 2 3 y 4 5 y 6	1	30
	Integridad de sistemas informáticos	- Inutiliza - Impedir acceso - Entorpecer su funcionamiento	7 8 9	1	30

Fuente: cuestionario

Índice de valoración 1= Totalmente en desacuerdo 2 = En desacuerdo 3 = Ni de acuerdo ni en desacuerdo 4 = De acuerdo 5 = Totalmente de acuerdo

Especificaciones del cuestionario sobre lel derecho fundamental a la intimidad personal.

Variable/Dimensiones		Indicador	Item	Puntaje Mínimo	Puntaje Máximo
Derecho fundamental a la intimidad personal	Intimidad	- Personal - Dignidad - Espiritual	1 y 2 3 y 4 5	1	30
	Privacidad	- Prácticas sexuales. - Condiciones de salud. - Comunicaciones personales	6 y 7 8 9 y 10	1	30
	Reserva	- Información - Propiedad - Libertad de conciencia	11, 12 y 13 14 15 y 16	1	30

Fuente: cuestionario

Índice de valoración 1= Totalmente en desacuerdo 2 = En desacuerdo 3 = Ni de acuerdo ni en desacuerdo 4 = De acuerdo 5 = Totalmente de acuerdo

ANEXO 4

CUESTIONARIO

APLICABLE A LOS MAGISTRADOS DEL PODER JUDICIAL

El presente formato tiene por finalidad recoger información en las unidades de población: Jueces y Fiscales Penales del Distrito Judicial de Puno de nuestra Tesis titulada EL DELITO CONTRA DATOS INFORMÁTICOS PERSONALES EN EL DERECHO FUNDAMENTAL A LA INTIMIDAD PERSONAL EN LA CORTE SUPERIOR DE JUSTICIA PUNO 2020, La reseñada encuesta es de perfil anónimo, así como la gentileza por brindar su tiempo al presente Cuestionario.

DATOS GENERALES

Sexo: Masculino ( ) Femenino ( )

Magistrado: Poder Judicial ( ) Ministerio Público ( )

VARIABLE INDEPENDIENTE "EL DELITO CONTRA DATOS INFORMÁTICOS PERSONALES"						
ITEM	**PREGUNTA**	**Totalmente en desacuerdo**	**En desacuerdo**	**Ni deacuerdo, ni en desacuerdo**	**De acuerdo**	**Totalmente deacuerdo**
1	Acceder en forma deliberada a un sistema informático afecta la intimidad de la persona.					
2	Acceder a un sistema informático en forma deliberada afecta la privacidad de la persona.					
3	Acceder en forma ilegitima a un sistema informático afecta la reserva de la persona.					
4	El acceder a un sistema informático sin autorización esta sancionado por ley.					
5	El ingresar a un sistema informático vulnerando el sistema de seguridad afecta a la privacidad de la persona.					
6	Cuando alguien ingresa a un sistema informático vulnerando su sistema de seguridad debe ser sancionado penalmente.					
7	Dejar inutilizable un sistema informático perjudica el patrimonio de una persona.					
8	Impedir el acceso a un sistema informático vulnera el derecho a la información.					
9	Cuando una persona entorpece el funcionamiento de un sistema					

	informático retrasa el trabajo.					
VARIABLE INDEPENDIENTE "DERECHO FUNDAMENTAL A LA INTIMIDAD PERSONAL"						
ITEM	**PREGUNTA**	**Totalmente en desacuerdo**	**En desacuerdo**	**Ni deacuerdo, ni en desacuerdo**	**De acuerdo**	**Totalmente deacuerdo**
1	El derecho a la intimidad es la protección de un acto personalísimo.					
2	Los actos personalísimos son privados y reservados					
3	La trasgresión de un acto personalísimo afecta la dignidad de una persona.					
4	La dignidad se encuentra protegida constitucionalmente.					
5	Existen actos espirituales que son protegidos por el derecho.					
6	Las imágenes sobre prácticas sexuales son privadas.					
7	La divulgación de información sobre prácticas sexuales menoscaba la intimidad de la persona.					
8	La divulgación de la información contenida respecto a las condiciones de salud afecta al derecho de privacidad.					
9	La intromisión a las comunicaciones personales, menoscaba la libertad de comunicación.					
10	La interferencia de las comunicaciones personales esta sancionado penalmente.					
11	La Información es un conjunto de datos.					
12	La información personal esta considerada como reservada.					
13	La divulgación de la información personal sin consentimiento es un delito.					
14	Toda información respecto a la propiedad de una persona es protegida a través de la reserva de propiedad.					
15	La libertad de conciencia está considerada como el conocimiento o saber que tiene una persona de algo.					

16	Toda persona tiene derecho a la libertad de conciencia.					