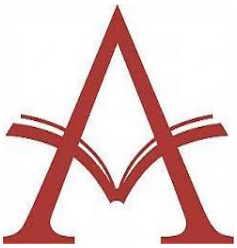
UNIVERSIDAD PERUANA DE LAS AMÉRICAS



ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACIÓN

La Evidencia Digital y los Delitos Informáticos en el Sistema Jurídico Peruano, 2020

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

AUTOR: GALLEGOS OSORIO, SIGFREDO ANTONIO

CÓDIGO ORCID: 0000-0003-1289-8420

ASESOR:

Dr. QUISPE DIAZ GILBER CARLOS

CÓDIGO ORCID:

0000-0002-1515-2491

LÍNEA DE INVESTIGACIÓN: DERECHO PENAL, CIVIL Y CORPORATIVO

LIMA, PERÚ

Febrero, 2022

RESUMEN

A raíz de los constantes avances en la información, tecnología y en el mundo de las comunicaciones, nos debemos dar cuenta cómo la tecnología influye en nuestras vidas y acciones día a día.

El presente trabajo presentará las condiciones que se deben tomar en cuenta en la revisión de las pruebas digitales y cómo se deben utilizar en los procedimientos judiciales, Así como, lo relacionado al cibercrimen, la Convención de Budapest, los criterios internacionales y nacionales referentes a este tema. También, las pruebas obtenidas y las evidencias digitales en el proceso.

El perfil del ciberdelincuente ha cambiado notoriamente, antes era aquel sujeto perito en computadoras que se inmiscuía en aspectos confidenciales y en la mayoría de los casos los fines siempre son económicos.

La investigación se enfocará en los delitos cibernéticos y las medidas tomadas de parte del Estado peruano y de la regulación de otros países.

Palabras clave: Debido proceso, intimidad, ciberdelincuencia, cibercrimen.

ABSTRACT

As a result of the constant advances in information, technology and in the world of communications, we must realize how technology influences our lives and actions every day.

This work will present the conditions that must be taken into account in the review of digital evidence and how they should be used in judicial proceedings, the relationship of digital evidence with the principles of legality, probation and the right to freedom was reviewed. privacy. As well as, what is related to cybercrime, the Budapest Convention, the international and national criteria regarding this issue. Also, the types of evidence that can be obtained and the digital evidence in the process.

The profile of the cybercriminal has changed notoriously, before it was that subject expert in computers that intrudes in confidential systems as a personal challenge, now the crimes of fraud, violation of privacy, extortion and others can be committed by people with computer knowledge basic and the ends are always economic.

The investigation will focus on cybercrimes and the measures taken by the Peruvian State and the regulation of other countries.

Keywords: Due process, privacy, cybercrime, cybercrime.

TABLA DE CONTENIDOS

I.- INTRODUCCIÓN

Con la tecnología de comunicación ha aumentado la incidencia negativa en los medios digitales, y trae consigo un problema mundial donde delincuentes utilizan este medio para realizar acciones criminales.

En este caso las pruebas o evidencias quedan grabadas en el sistema digital para presentar una responsabilidad penal en cualquier circunstancia. A este respecto, las pruebas deben realizarse con personal adecuado para lograr su recuperación y buscar la validez del delito cibernético ocurrido.

Para lograr esto se debe consolidar una relación estrecha entre la sociedad y el Estado, para tal efecto, es importante conocer las herramientas digitales actuales y buscar profesionales calificados, de esta manera obtener información contenida en las redes sociales.

La investigación enfoca el tema de la tecnología como un derecho de libertad, intimidad que la delincuencia no respeta.

II.- ANTECEDENTES

2.1.- Nacionales

- Aliaga (2019), en su tesis titulada: "La incidencia de los delitos informáticos en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022", presentada en la Universidad las Américas. El autor llegó a la conclusión que los delitos informáticos están estipulados negativamente en el proyecto de OSITRAN.

- Ramos (2020), en su tesis titulada: "Factores procesales en el archivamiento de los delitos informáticos, vistos en la primera y segunda fiscalía provincial penal corporativa de Leoncio Prado, 2017-2018", presentada en la universidad de Huánuco. El autor llegó a la conclusión que es sumamente importante y necesario crear un espacio adecuado para los delitos cibernéticos recientes.

2.2.- Internacionales

- Merino (2017), en la tesis titulada: "Delitos informáticos y las salidas alternativas posibles revisadas desde el análisis económico del derecho", presentada en la Universidad de Chile, Se ha establecido como objetivo estudiar la ley donde el Estado interviene en el marco del convenio de Budapest. El autor concluyó que es una alternativa de solución para reducir el trabajo tribunal y del ministerio público.

- Prieto y Vargas (2020), en su tesis titulada: "Ciberdelincuencia, enfocada en la apropiación de información a través de medios electrónicos y su influencia en el

cometimiento de delitos informáticos", establece que los autores concluyen que el desconocimiento y poca o nula preparación de expertos en temas de infraestructura y equipos tecnológicos son causas del avance de los delitos informáticos en su país.

III.- BASES TEÓRICAS

3.1.- Doctrina

3.1.1.- Evidencia digital

De acuerdo con Sergi (2018) citado por Del Valle (2018), estableció que existen diferentes opiniones sobre el concepto de prueba digital. Esta cuestión fue considerada desde diferentes puntos de vista y por diferentes organizaciones, las cuales presentaron diferentes propuestas, teniendo en cuenta sus propias características.

Casey (2011) citado por Del Valle (2018), cuya evidencia digital se use o almacene en un dispositivo técnico donde se verifique la evidencia o la participación en un delito, como la intención o la posibilidad de manipulación o coartadas

Fases

Son: Diseño de prueba, producir registros, reunir evidencia, analizar la evidencia e informes y presentación.

Fuentes

Los lugares donde se almacena la evidencia digital son en las computadoras, en la memoria de acceso aleatorio (RAM), si esto se hace en la red ahora es bastante posible. Para ello, los datos de las evidencias digitales son:

a. Sistema de computación abierta:

Son las laptop, y los servidores.

b. Sistemas de comunicación:

Relacionado con redes de telecomunicaciones, comunicaciones inalámbricas e Internet**.**

Sistemas convergentes de computación:

Celulares de alta gama, PDAs, tarjetas inteligentes.

Características

1. Volátil
2. Duplicable
3. Alterable y modificable
4. Eliminable

Lugares en que se encuentra la evidencia

1. Dispositivos de almacenamiento informático
2. Dispositivos portátiles
3. Dispositivos periféricos
4. Redes de computadoras

La evidencia digital en el derecho comparado

Cabe señalar que el surgimiento de nuevas tecnologías en nuestra sociedad es un tema que tiene un impacto integral en todos los sistemas legales del planeta, especialmente en los países desarrollados, por lo que debe estar disponible a escala global.

Los lugares donde se almacena la evidencia digital son en las computadoras, en la memoria de acceso aleatorio (RAM), si esto se hace en la red ahora es bastante posible. Para ello, las fuentes de evidencia digital.

Al hablar de legislación comparada sobre prueba digital, es necesario mencionar las diferencias digitales que existen de un país a otro, lo que lleva a que el tema de la prueba digital como prueba en las sesiones, y la vía penal quede incompleta.

Por ejemplo, en España cuentan con documentos electrónicos como prueba. En Francia, promulgó una legislación donde después de las 6 de la tarde habilita a sus empleados sin correos o mensajes, ofreciéndoles desconectar sus teléfonos inteligentes y computadoras portátiles (Bes, 2014) citado por Del Valle (2018).

En Colombia, en 1999, el gobierno promulgó la ley 527 que acredita los documentos electrónicos. En EEUU. Muchos jueces determinan en la dirección de IP no es identificable, este lugar es insuficiente para acreditarla a una persona, ya que, la persona que originó esa información no es necesariamente la misma del IP (Bes, 2014) citado por Del Valle (2018).

En Argentina están obligados a mantener los libros contables en papel.

Por las opiniones diversas en los diferentes países del planeta y para unificar normativas jurídicas se realizó la Convención de Budapest.

En la Convención de Budapest, tiene 48 artículos; donde manifiestan conceptos, recomendaciones, cooperación internacional, escenarios de apoyo entre los gobiernos y acciones de investigación.

Relación en el debido proceso

Un juicio justo se enfrenta a un nulo normativo en la materia, estableciendo que es necesario buscar alternativas al juicio donde se respeten los derechos del imputado a través de documentos.

Relación en el principio de libertad probatoria

La prueba digital en la Ley de Procedimiento Probatorio está vinculada al principio de libertad de prueba. Pero a pesar de esto, existen limitaciones consagradas en la constitución y los derechos humanos.

Con ello, garantiza que el Estado no puede hacer cualquier cosa por buscar la verdad, amparándose en investigaciones ilícitas graves.

Relación en el principio de *nulla coactio sine lege*

Para Bruzzone y Bertolino (2005), presenta la diferencia entre medios probatorios y las medidas de coerción probatoria.

Este tema establece un obstáculo a su legitimidad, ya que toda actividad con la finalidad de conseguir materiales probatorios, llevados a cabo con coerción.

Relación en el derecho a la intimidad

En estos años, se ha acrecentado información en formato electrónico es muy grande y trascendente, por lo que los gobiernos deben desarrollar estrategias para hacer valer la privacidad, tanto en materia de ciberdelincuencia y prueba técnica, como prueba en procesos penales.

Dominio probatoria de la evidencia digital

En el pasar del tiempo, los contextos en intimidad personal, conocido antes a cambiado ahora tiene un aspecto más amplio y relaciona los sistemas informáticos y las redes sociales.

Sistemas de valoración de la prueba

Para Cafferata Nores (1998), evaluar la evidencia como: evidencia forense, fe íntima, crítica racional.

Principios rectores de evidencia digital

- La relevancia se relaciona solo a los documentos o pruebas relacionados a lo investigado para probar o rechazar sustentos legales.
- La confiabilidad valida la autenticidad del proceso porque pueden ser analizados en toda ocasión.
- La suficiencia relacionada con las pruebas las cuales validan la investigación. Este tema también se relaciona con la experiencia del perito.

Medios electrónicos:

Correo electrónico. - Existen dos evidencias digitales en este aspecto: física y electrónica, para cada una de las cuales se requiere un informático y un notario. Cuando se presenta la prueba, los peritos deben estar presentes.

Imagen digital. – Las fotos digitales brindan datos confiables, que se reflejan cuando se ingresa la propiedad del archivo, como el día y el momento en que se tomó, el dispositivo utilizado y más. La evidencia digital se representa en imágenes digitales tanto en forma física como electrónica.

La evidencia en la nube. - Según Koops & Goodwin (2014), citado por Del Valle, (2018), este modelo permite que todos los datos se guardan en la nube que son mencionados como proveedor del servicio.

Celulares inteligentes. Constantemente los teléfonos inteligentes están perfeccionándose y con ello también se debe actualizar los mecanismos de conocimiento de tales avances.

Validez jurídica de la evidencia digital

Para que una evidencia sea considerada como una prueba, es necesario que esta cumpla con ciertas características:

a) Admisible.

Cano (2006) citado por Puga (2,019), se ha establecido que las personas jurídicas realizaron el análisis sobre la base de: originalidad, confiabilidad, exhaustividad y criterios legales. Todo lo que sirva de prueba debe obtenerse sin vulnerar los derechos y garantías constitucionales, autenticidad.

Los documentos aprobados deben presentarse en cada proceso y en los equipos y en los archivos fotográficos firmados por la persona responsable. Además, los materiales relacionados con el crimen se seleccionan de la escena del crimen.

Solo cuando se usen los mecanismos y tareas que vigilan la integridad se puede reducir los riesgos de manipulación de evidencia.

b) Completa.

El perito analiza las medidas para conseguir el material adecuado que será probatorio para esclarecer el crimen.

c) Confiable.

La información de donde se obtiene la información debe ser creíble y verificable.

d) Creíble.

Los técnicos encargados de la redacción de documentos, donde se explica la evidencia del caso deben explicarlo de manera sencilla para que los jueces lo entiendan.

e) Precisión.

Las etapas de recojo, análisis y manejo de evidencia debe ser claro para lograr no perder evidencias o que estas se maltraten en el camino o tiempo.

f) Suficiencia.

El escenario que se debe mostrar en el caso debe ser completo, sin sesgo para lograr el éxito de la investigación.

g) Relevancia.

El valor es el elemento principal de este criterio, dentro de la investigación.

3.1.2.- Delitos informáticos:

Origen de la palabra delito:

Para Moreno (2001) citado por Daza (2012), Se informa que el significado de "delito" se refiere a un acto ilegal y malicioso sujeto a castigo. Se recibe en diversas formas físicas o psicológicas y está penado por la ley.

Según Camacho (1987) citado por Acurio, (2017), explica que en la convivencia entre los hombres hay engaño, manipulaciones, codicia, ansia de venganza y fraude, acciones donde impera el delito.

Concepto de falta:

Vega (2010) citado por Cárdenas y Lazo (2014), considera el delito menor, doloso o menos grave.

Diferencia entre Delito y Falta

En muchos países se presenta la clasificación de delito y contravenciones o faltas. Para Rodríguez (1995) citado por Cárdenas & Lazo (2014), señala que las acciones que la ley penaliza son el delito y aquellas que son infracciones a la ley son penas leves.

Teoría General del Hecho Punible

Zaffaroni (1991) citado por Cárdenas & Lazo (2014), señala que el derecho penal estudia la conducta punible, y estudia y explica aspectos similares de la conducta punible; Tiene la intención de cometer una falta o delito.

Principales elementos de los hechos punibles:

a. **Conducta.** Zaffaroni (1991) citado por Cárdenas & Lazo (2014), menciona que los delitos hechos punibles solo se relaciona al ser humano ya que él es el agente vivo con sentido y raciocinio.
b. **Tipicidad.** - Peña (1994) citado por Cárdenas & Lazo (2014), señala que la tipicidad es un hecho abstracto, todas las acciones son punibles siempre que no estén previstas en la ley.
c. **Antijuricidad o antijuridicidad.** – la tipicidad no es principal característica de una conducta, ya que no necesariamente sean unas conductas típica establecida en una falta o delito. Paco (2000) citado por Cárdenas & Lazo (2014), precisa que la tipicidad es antijuricidad. Esto quiere decir que es contrario al ordenamiento jurídico y distinto a las normas sociales.
d. **Culpabilidad.** la antijuricidad no necesariamente es un hecho penado. Cresu (1999) citado por Cárdenas & Lazo (2014), menciona que la pena es una consecuencia congruente a la responsabilidad subjetiva, los culpables, han realizado alguna actividad fuera de la ley y a pesar de estar prohibido lo llevó a cabo con conocimiento de ello.

Definición

Acurio (2017), define un delito informático como un acto ilícito que podría, en algún momento, ser considerado un delito, cuya finalidad es solucionar un problema o instigar un conflicto.

Según López (1994) citado por Daza (2012), determina que el delito informático se define como un delito en el que se utiliza un sistema de procesamiento electrónico de datos como herramienta o interceptación, se manifiesta de muchas formas y lesiona intereses legítimos. (p. 29).

Para Moreno (2001) citado por Daza (2012), los delitos relacionados con una computadora son acciones cuyos casos la computadora es el objetivo, en otros es un instrumento para llevar a cabo la acción ilícita.

Tipos

La mayoría de autores presenta dos tipos principales de delitos, que enmarca instituciones públicas o privadas, las cuales son:

-Delitos de alta tecnología

INTERPOL señala que el Cibercrimen refiere a todo ataque sofisticado contra el hardware y software, cuyo objetivo es ingresar sin permiso a un dispositivo.

Para la INTERPOL Crimen amplificado, se refiere a todo delito 'tradicional' como delitos diversos.

Características Delitos Informáticos

Según Téllez (1997) citado por Cárdenas & Lazo (2014), menciona:

a. Son conductas criminales de cuello blanco, personas con información ocasionan estos delitos.

b. Actividades de oportunidad, toma la razón de tecnología y economía.

c. Tareas profesionales, el sujeto se encuentra laborando.

d. Ocasiona pérdidas económicas, produce a las personas involucradas.

e. Otorga facilidades relacionado con e tiempo y espacio, porque se puede consumir rápidamente y sin presencia física.

f. Los casos aumentan, pero son pocas las denuncias, ocasionado por la limitada regulación en relación al derecho.

g. Están relacionados a la actividad militar.

h. La comprobación es difícil, por su carácter técnico.

i. Los menores de edad tienen facilidades.

j. Aumentan cada día más.

Sujetos

a. Sujeto Activo

El imputable se establece en aquella persona natural, no un delincuente común, es hábil en el manejo de la tecnología y, por lo tanto, en los lugares de trabajo donde la información es importante.

b. Sujeto Pasivo

Son personas naturales o jurídicas, que necesita información.

3.2.- Legislación

Legislación Peruana

En el Perú, D. L. N. 635°, Capítulo X:

- Artículo 207-A.
- Artículo 207-B.
- Artículo 207- C.

En el Código Penal peruano (CP), entre los delitos contra la confianza pública, rigen la falsificación y estafa de imágenes digitales.

Nueva Ley 30171, modifica la Ley 30096 Ley de Delitos Informáticos.

- Delitos contra la información y sistemas informáticos (Capítulo II) siendo este diseñado por formas penales: Artículo 2 (acceso indebido), Artículo 3 (vulneración de la integridad de los datos informáticos) y Artículo 4 (vulneración de la formación del sistema de información).
- Violación informática perjudicando respuesta y la libertad sexual (Capítulo III) se incluye la Sección 5 (Sugerencias sexuales a niños y jóvenes con fines mediante tecnología), penalizando la sugerencia sexual (solicitando y obteniendo material sexualmente explícito, realizando acciones sexuales) a niños y adolescentes que usan tecnología.
- Delitos Informáticos Contra la Privacidad y Confidencialidad de las Comunicaciones (Capítulo IV) Este capítulo incluye las siguientes sanciones: Artículo 6 (repetidas por la Ley 30171, Reparación de la Ley 30096, Derecho del Delito) y Artículo 7 (Marcando datos informáticos).

- Delitos Informáticos Contra la Propiedad (Capítulo Quinto) Este capítulo incluye la Sección 8 (Fraude Informático) que sanciona la creación, inserción, modificación, borrado, borrado y copia de datos informáticos que provoquen perturbaciones desfavorecedor de terceros.
- Violación Informática Contra la Confianza Pública (Capítulo VI), Artículo 9 de la Ley (Asignación de Identidad) sanciona la apropiación de la identidad de una persona física o jurídica, siempre que cause daño.
- Disposiciones frecuentes (Capítulo Séptimo): está compuesta por los siguientes delitos: Artículo 10 (uso indebido de computadoras y mecanismos) y Artículo 11 (circunstancias agravantes).
- Sanciones introducidas por el regulador a las personas jurídicas La nueva ley de ciberdelincuencia incluye las últimas 11 cláusulas adicionales, nos centraremos únicamente en los individuos, que se encuentran en DCF de nueva ley.

Reformas del Código Penal dependidas con los delitos informáticos

Los artículos 158, 162 y 323 del Código Penal fueron modificados por el artículo 4 de la ley 30171 (Ley que modifica la Ley Nº 30096º, Ley de delitos informáticos) en los siguientes términos:

> "Artículo 158.- Los delitos previstos en este capítulo son perseguibles por acción privada, salvo en el caso del delitos previsto en el artículo 154-A

Esta sección, se establece la descripción, del procedimiento de privacidad para los esquemas cubiertos en el Capítulo II de Invasión de la privacidad. A partir de la adición de la Cláusula 154-A Tratamiento Ilícito de Datos Personales, la causa penal general queda prevista únicamente para la sentencia conjunta antes mencionada.

> "Artículo 162.- 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, inciso 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 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 años cuando el delito comprometa la defensa, la seguridad o la 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".

En el presente artículo ha sido revisado en la composición lo antepuesto era demasiado amplia y dejaba a la discreción del fiscal general decidir qué los datos debería considerarse clasificada, guardada o reservada. Esta es la claridad de las circunstancias agravantes de la interferencia telefónica cuando afecta los datos de confidencial, privada o secreta en esta se encuentra la Ley 27806 Ley de Transparencia y Acceso a la Información Pública.

Debe entenderse que al mencionarse con posterioridad a la sanción de la Ley 30096, el 5 de diciembre de 2013, introdujo el Proyecto de Ley 3048/2013-CR, con autorización para mejorarla dicho precepto, con la sospecha de que no estaba adecuadamente descrito en términos de conducta. También fueron sancionados con una serie de agravantes como el móvil del delito.

> "Artículo 154-A.- El que ilegítimamente comercializa información no publica relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análogo sobre una persona natural, será reprimido

> con pena privativa de libertad no menor de tres ni mayor de cinco años. 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 el párrafo anterior".

El delito de tráfico ilícito de datos personales prevé una sanción por la comercialización (comercialización, comercio, venta, promoción, promoción o facilitación) de datos desleales, sean o no nocivos dichos actos.

Este delito se caracteriza porque manifiesta una especie de disposición interior trascendente, que presenta elementos subjetivos denotando una determinada intención que incluye la búsqueda de un determinado resultado. Se requieren resultados extraordinarios, lo que se considera cortante. Resultados, porque el agente busca un resultado más allá del tipo de base de datos de marketing, procesamiento, etc. Ejemplo: Base de datos de marketing con nombre, identidad, edad, estado civil, dirección, número de teléfono, trabajo, ocupación, salario, etc.

> "Artículo 183-B.- El que 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. 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".

Esta determinación ha sido penada con castigar el contacto (establecer contacto o comunicarse) con un menor para solicitar u obtener materiales pornográficos o para participar en actividades sexuales. Se decidió que esta figura prevé ocurrencias agravantes cuando la

víctima tenga de catorce años a menos de dieciocho años y cometa un hecho doloso, en cuyo caso la pena no será también inferior a tres años.

Determinando que esta imagen delictiva (sugerencia de sexo para niños y adolescentes), por las descripciones dadas por la categoría jurídica, la cataloga como una especie de esencialismo diferencial, pues establece en el elemento subjetivo que representa un intento particularmente consistente de buscar una resultado diferente al que normalmente se busca, lo que generalmente se clasifica como una violación del resultado de trituración, porque los gránulos organizados buscan un resultado más allá de la categoría, a saber, obtener material sexualmente explícito o participar en actos sexuales con un menor de edad.

Legislación Internacional

A nivel internacional, hay diferencias entre los países, tomando como eje, por ejemplo: EEUU., Gran Bretaña, Alemania y países nórdicos, prevalece la libertad de prueba, los juzgadores valoran medios de prueba. A diferencia de Francia, Bélgica e Italia, donde prevalece la ley de la prueba escrita.

El Estado de UTAH fue el primero en regular un nuevo uso en la autopista informática. La Ley de la Firma Digital de UTAH, fue un referente a nivel nacional, y en 1995 se publicó la Guía de Firma Digital; en el 2000 se aplicó la primera ley nacional sobre firmas digitales, dando el mismo valor legal escrito en papel.

En Italia, desde 1997, la legislación italiana se rige por reglamentos, documentos y contratos, en el capítulo 1, artículo 5 y 12 hace referencia a la regulación de documentos informáticos.

En Francia, en 1980, país pionero en este tema, como estipula el artículo 1315 y 1316 (1, 2 y 3).

3.3.- Jurisprudencia

Los Hechos

Entre el 28 de diciembre de 2001 y el 8 de enero de 2002, un ex empleado de la empresa chilena ATI cometió una serie de acciones ilegales para interferir en su servidor, modificando, destruyendo y conociendo la información contenida en el mismo. Las páginas relacionadas son: www.guestbook.cl y www.metabuscador.cl

Camp era un joven de 19 años, contactado en la conversación de IRC como "P0key", que supuestamente lo hizo para vengarse de la empresa por haber sido despedido de la empresa. Los crackers piratearon ilegalmente estos sitios, modificaron el contenido, crearon un nuevo sitio (index.html) que reemplazó al sitio actual, mostraron mensajes ofensivos a la empresa y nos dijeron que la página estaba pirateada.

Los administradores del sistema informático decidieron realizar acciones inmediatas, y verificar todas las memorias de servidores y pueden verificar que estos sitios se han hecho de un ataque desde la cadena Sneak, y luego elimine algunos archivos de negociación. Cuenta FTP, para eliminar los efectos en términos de ataques. Aunque la auditoría fue en realidad, es posible verificar que " cracker" intente ingresar el correo electrónico de la compañía, que se puede verificar de inmediato.

Compruebe el 90% de los ataques de una dirección IP estática, que corresponde a una red de café de red que lo acusa luego, como administrador. Otros ataques provienen de la transferencia de cuentas de acceso a Internet, principalmente desde el hogar de convicciones.

Estableciendo una investigación y presentando una denuncia de denuncia de investigación informático, este caso atrajo la atención de la prensa se intereso en el tema, entre los usuarios del chat de IRC. Teniendo esta oportunidad de ese momento, el imputado publicó voluntariamente el diario El Centro de Talca y concedió una entrevista, colocándola en primera plana con el titular: “Soy un pirata electrónico”. De esta forma ganó fama y reconocimiento por

parte de sus compañeros, hecho por el cual muchas veces se buscaban "crackers". Incluso se hace publicidad para reparar sistemas de seguridad en el sistema.

El Juicio Abreviado

Al comienzo de la jornada del juicio, se hicieron los preparativos para el juicio oral, y se realizaron las intervenciones: el Fiscal General, el Abogado General de los Delitos y el Fiscal acordaron proceder según el proceso abreviado. Se establece que el acusado debió de renunciar a dos delitos más para poder efectuar con los requerimientos establecidos en el Código Procesal Penal. Después de hacer puntualizadas preguntas al procesado, el magistrado de fianzas, Marta Asian Madariaga, realizó un juicio sumario, despejó el camino para que el fiscal presentara el caso. El fiscal de la ciudad de Talca, señor Carlos Olivos Muñoz, se pronunció sobre los hechos, la investigación realizada y todas las pruebas reunidas durante los 8 meses de estudio y pidió la pena de 3 años de prisión. Establecidos en los artículos 1, 2 y 3 de la Ley 19.223.

El querellante, abogado Alberto Contreras Clunis, resumió en que ha destacado por el fiscal general explicando la seriedad de los presuntos autos, describiendo daños causados también en la empresa y el dolo el imputado. Del cual se establecido la aceptación del imputado de participar en su declaración a la policía y alardear durante el interrogatorio con el periodico El Centro. Se debe determinar la inclusión de un informe que incluya un especialista en peritaje en la Brigada de Ciberdelincuencia de la Policía de Investigaciones de Chile. Efectivamente, se desarrollo un escaneo en la computadora del autor estaba usando dentro de las instalaciones del Cibercafé, y también en su computadora personal. Gracias al complejo sofware realizado en esta oportunidad, es posible acceder a datos perdidos o archivos borrados del disco duro de la CPU en Cyber Café. Una persona merece atención especial, incluido un correo electrónico que el Demandado le envió a su socio diciéndole: “Estoy eliminando a una cantidad de personas

(“weas”) que podrían perjudicarme en asuntos legales…”, enviado exactamente la tarde anterior a la persona que denuncia a la policía.

Las averiguaciones han señaló en sus definiciones profesionales que: "La computadora en cuestión tiene las capacidades técnicas necesarias y el software apropiado para navegar por Internet y dañar un sistema informático. De hecho, se identificó que el disco duro contenía 24 programas: "... por piratas informáticos, vándalos o delincuentes informáticos". El demandante concluye destacando los avances en tecnología informática en nuestros tiempos, se debe tener en cuenta el daño tanto a las personas como a las empresas, que pueden llevar a la quiebra económica. Por la pérdida de reputación como consecuencia de estos delitos, se sancionará con 5 años de prisión, artículos 1, 2 y 3 de la Ley 19.223.

Por su parte, el fiscal general de la Corte, Joaquín Lagos León, dijo y explicó que no había pruebas de que su defendido estuviera involucrado en los casos, al tiempo que negó la veracidad del informe policial. Sentó un nuevo precedente en la legislación norteamericana según el cual las empresas que prestan servicios de seguridad informática y las personas "hackeadas" serán multadas por no cumplir con sus servicios.

Específicamente sobre esta situación personal del acusado, alegando que es un joven autodidacta que ha hecho un gran esfuerzo, es padre de familia y tiene una familia. A cambio, pidió que su defendido sea absuelto y en caso de condena, la aplicación de la medida mínima, es decir, una pena de 541 días de prisión, acompañada de libertad condicional, para no poner firma de antecedentes penales.

El Fallo

Al término de la audiencia, el juez de libertad condicional resolvió: Violación de las Leyes N° 19223 N° 1, 2 y 3, fijándose el 11 de abril de 2003 como fecha de su sentencia, consistente en 13 autos. Analiza minuciosamente toda la evidencia para determinar la descripción exacta del crimen y cómo se determinó.

Al imponer la pena, el juez advirtió que en el caso de una reincidencia, la única pena prevista en los artículos. 351 del CPC. También cabe señalar que el inciso del cuarto párrafo del artículo anterior dice: "competencia del tribunal" ya que el actor exigió una pena más severa para el actor. Por otro lado, ofrece: El conjunto de atenuantes no nos convence, pues son, según lo identificado, reincidencia, y se les aplica la pena en la medida señalada, y se considera más adecuada. . la conducta ilícita del imputado. En respuesta, se impone una pena de tres años y un día, que es la pena mínima máxima de prisión para menores de edad.

Comentarios

La complejidad determina si se trata o no de un delito informático. Sin embargo, la claridad de la sentencia nos da plena confianza en que el tipo de delito y sus consecuencias se entienden cabalmente. A veces, la evidencia pericial es importante para revelar la verdad y la participación del perpetrador en estos delitos, lo que se entiende completamente determinando, la razón en su desarrollo valeroso.

Además, es importante como punto que se encontrara la CPU y el servidor del cibercafé del acusado, que ayudó a descubrir a través de un análisis exhaustivo; Puede especificar los días, horas, minutos y segundos en que se realizaron los ataques, de dónde provinieron de la persona que lo desarrollo. El rápido accionar bloquearon cualquier intento de daño mayores implementadas en las oficinas de sistemas de la empresa. En coordinación del Fiscal de Talca,

Carlos Olivos, la querellante y el abogado de la víctima, diseñaron una investigación que, a lo largo de ocho meses, arrojó gran cantidad de pruebas contundentes delito acusado.

Dado que este es el primer caso de delito informático que se fija en un proceso penal y se aclaran las razones de la condena, necesariamente se convertirá en un precedente vinculante.

La trascendencia de este caso, además su Sentencia exitosa, para el agraviado que ha atrevido a manifestar un delito, teniendo como los resultados la protección de clientes y su reputación, la empresas en general no sean víctimas de estos crímenes. Finalmente, se puede ver simplemente mostrando que actualmente existe la tecnología suficiente para investigar este tipo de delitos y por lo que sería mejor castigar a los autores de estos delitos, lo que erróneamente se denomina "Fideicomiso", hacker" es, estrictamente hablando, una simple computadora y delicuentes.

3.4.- Tratados

Los únicos estándares internacionales incluyen leyes sobre delitos y cooperación internacional. Esta es la primera herramienta y uniforme hasta ahora. Como la amenaza de redes utilizando redes de tecnología para participar en pruebas almacenadas y no legítimas y entregadas por redes; De manera similar, la colaboración de los gobiernos y el rubro privado que esta vigilante en los delitos electrónicos, es necesario para abordar los intereses reales y aumentar esto; Se establece que la efectividad de estas ofensas informáticas, requiere el establecimiento de una serie de cooperación internacional para intercambiar reglas legales y oportunas y operativas; En otras palabras, la verdad es contraria a la seguridad, la autenticación y la autorización de los sistemas de información, las redes y los datos informáticos, así como el reconocimiento de las autoridades apropiadas para combatir la eficiencia de la red social, lo que lo ayuda a explorar. Y su investigación y su mente, a nivel nacional e internacional.

La Convención cibercriminalidad se centra en tres buenos objetivos buenos, la primera persona para el derecho penal, el segundo grupo de medidas de procedimiento y, finalmente, considerando una cooperación internacional graciosa y efectiva. Investigaremos determinados Acuerdo de Ciberdemes Budapest (2001) en el Artículo 14. 1 y 2, describe: el desarrollo de su regulaciones de proceso. Determinación la implementación de medidas legislativas y otras medidas siendo importante para desarrollar y ejecutatar previstos para esta determinar el grado de estudio y su determinado proceso penal (...) "Bedapest Cybercrime Convention Article (2001). Párrafo 201. Para los registros de datos en el momento real, las partes aplican nuevas leyes y lo que necesitan y sus poderes se pueden exportar o mantener mediante el uso de compuestos de computadora encontrándose en su nación. Ciberdelincuencia Budapest (2001) en el Artículo 22 Digital 1 Organización: "Jurisdicción. Determinar en la nación debe, en su jurisdicción, establecerse frente a cualquier acto ilícito (…), en su propio país, a bordo de cualquier transporte (…)".

El Convenio de Budapest sobre el Delito Cibernético (2001) establece en el Artículo 23: "Principios generales relacionados con la cooperación internacional. Las Partes cooperarán en la mayor medida posible en la aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal y acuerdos basados en leyes uniformes o recíprocas compatibles con las disposiciones de este Capítulo, sus estatutos, con fines de investigación o procedimientos relacionados con un delito relacionado con los sistemas y datos informáticos o para obtener pruebas electrónicas de un delito." El Convenio de Budapest sobre Ciberdelincuencia (2001) establece en el Artículo 25 No. 1 que los estados miembros deben ayudarse mutuamente en el contexto de las investigaciones u operaciones contra la ciberdelincuencia relacionadas con la protección de los sistemas y datos informáticos, así como la recopilación de evidencia digital de el crimen. El Convenio de Budapest sobre Delitos Cibernéticos (2001) establece en el Artículo 35: "Cada Parte designará un punto de contacto

disponible las 24 horas del día, los siete días de la semana, para garantizar que se brinde asistencia inmediata con fines de investigación o procedimientos penales relacionados con sistemas informáticos y datos, o para obtener evidencia electrónica de un delito tiende a facilitar o aplicar directamente los siguientes procedimientos, según lo permitido por la ley y la práctica interna: a) asesoramiento técnico b) retención de datos de conformidad con las Secciones 29 y 30, y c. recolección de pruebas, suministro de información jurídica y localización de los sospechosos". Conferencia Ciberdelincuencia Budapest (2001) en el artículo 37 de las normas digitales Nº 1: "Cumplimiento de la Convención. Después del impacto de este Convenio, el Comité Ministerial del Consejo de Europa, después de que los países consultores firmaron por la Convención y, una vez acordados, Acuerdo, esta convención podría ser invitada a cualquier Estado no es miembro del Consejo y que no esté involucrado en la construcción. La decisión se aplicó bajo la cual la ley de las restricciones del Consejo Europeo y con el voto endémico de representantes con la parte correcta del Ministro de Comité (...). Budapest (2001) en la Sección 46 Digital 1 a los Estados miembros que ejecutan una consulta continua para facilitar la interacción de la información legal o la tecnología de ciberdelincuencia y la prueba electrónica.

CONCLUSIONES

Primera: La evidencia digital influye significativamente los delitos informáticos en el Sistema Jurídico Peruano, 2020.

Segunda: La legalidad de la evidencia digital influye significativamente en los delitos informáticos en el Sistema Jurídico Peruano, 2020.

Tercera: El tratamiento jurídico procesal de la evidencia digital influye significativamente en los delitos informáticos en el Sistema Jurídico Peruano, 2020.

Cuarta: El soporte legal de la evidencia digital influye significativamente en los delitos informáticos en el Sistema Jurídico Peruano, 2020.

APORTE DE LA INVESTIGACIÓN

Primera: La investigación ofrece puntos de vista de diferentes países donde se realiza un proceso exhaustivo y claro de la ruta de la evidencia.

Segunda: Ofrece lineamientos generales para formular proyectos que se ajusten a las recientes necesidades nacionales.

Tercera: Se recomienda actualizar constantemente a su personal.

RECOMENDACIONES

Primero: El Ministerio Público tiene el papel de procurador de hacer cumplir la ley, para hacerlo más efectivo se debería crear una unidad específica.

Segundo: Se debe crear un cuerpo normativo específico.

Tercero: Se prepara un proyecto de ley que disminuya los delitos informáticos que existen en la red.

Cuatro: Nuestro país tiene mucho atraso en relación a la tecnología.

Quinto: Contratar profesional adecuado en relación a los crímenes informáticos ocurridos en nuestro país.

REFERENCIAS BIBLIOGRÁFICAS

- Acurio, d. P. (2017). Derecho penal informático. Obtenido de Pontificia Universidad Católica del Ecuador.
- Acurio, d. P. (2017). Derecho penal informático. Obtenido de Pontificia Universidad Católica del Ecuador
- Aliaga, S. A. (2019). La incidencia de los delitos informáticos en la implementación progresiva del plan de gobierno digital de OSITRAN 2019-2022. Obtenido de Repositorio de la Universidad Las Américas: http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/1127/ALIAGA%20SWIDIN.pdf?sequence=1&isAllowed=y
- Bertolino, Pedro, J, (200%). Bruzzone Gustavo A. Editorial Lexis Nexos. Abededo-Perrot, Buenos Aires, 2005, pág. 209.
- Cafferata Ñores (1986). La Prueba en el Proceso Penal con especial referencia a la VI 1 edición 1986
- Cárdenas, G. R., & Lazo, F. E. (2014). Delitos informáticos y el rol de la división de investigación de delitos de alta tecnología PNP, Lima, 2013. Obtenido de Repositorio de Centro de altos estudios nacionales: http://repositorio.caen.edu.pe/bitstream/handle/caen/67/1%20Caratula.pdf?sequence=1&isAllowed=y
- Daza, R. J. (2012). Análisis jurídico sobre los delitos informáticos en la legislación ecuatoriana. Obtenido de Repositorio de la Universidad Regional Autónoma de los Andes: http://dspace.uniandes.edu.ec/bitstream/123456789/2956/1/TUIAB001-2013.pdf

- Del Valle, L. D. (2018). Evidencia digital. Obtenido de Reositorio de la Universidad Empresarial siglo 21: https://repositorio.uesiglo21.edu.ar/bitstream/handle/ues21/16396/LOPEZ%20DANIELA%20DEL%20VALLE.pdf?sequence=1
- Espinoza, V. J., & Verdezoto, A. R. (2015). El rol de la auditoría forense ante los nievos delitos informáticos tipiicados en el actual código orgánico integral penal del Ecuador COIP, metodologías y herramientas a usar ante una evidencia digital. Obtenido de Repositorio de la Universidad Politécnica Salesiana sede Guayaquil: https://dspace.ups.edu.ec/bitstream/123456789/10348/1/UPS-GT001274.pdf
- Gómez, B. S. (2012). Metodología de la investigación. México: Red Tercer Milenio. Obtenido de R.
- Hernandez, D. L. (2009). El delito informático. Obtenido de EGUZKILORE: https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf
- Hernández, S. R., Fernández, C. C., & Baptista, L. M. (2014). Metodología de la investigación. Ciudad de México: Mc Graw Hill.
- Lasso, V. V. (2017). El estado el peritaje informático de la evidencia digital en el marco de la administración de la justicia en Colombia. Obtenido de Repositorio de la Universidad Nacional Abierta y a Distancia: https://repository.unad.edu.co/bitstream/handle/10596/17473/1113665550.pdf?sequence=1&isAllowed=y
- Merino, G. F. (2017). Delitos informáticos y las salidas alternativas posibles revisadas desde el análisis económico del derecho. Obtenido de Repositorio de la Universidad de Chile: http://repositorio.uchile.cl/bitstream/handle/2250/146816/Delitos-inform%C3%A1ticos-y-las-salidas-alternativas-posibles-revisadas-desde-el-an%C3%A1lisis-econ%C3%B3mico-del-derecho.pdf?sequence=1&isAllowed=y

- Monje, Á. C. (2011). Metodología de la investigación cuantitativa y cualitativa. Neiva: Universidad Surcolombiana.
- Prieto, V. N., & Vargas, C. (2020). Ciberdelincuencia, enfocada en la apropiación de información a través de medios electrónicos y su influencia en el cometimiento de delitos informaáticos. Obtenido de Repositorio de la Universidad de Guayaquil: http://repositorio.ug.edu.ec/bitstream/redug/50396/1/Nicole%20Prieto%20-%20Gladys%20Vargas%20BDER-TPrG%20019-2020.pdf
- Puga, R. R. (2019). La evidencia digital en los delitos de pornografía infantil. Obtenido de Repositorio de la Universidad Central del Ecuador.
- Ramos, C. K. (2020). Factores procesales en el archivamiento de los delitos informáticos, vistos en la primera y segunda fiscalía provincial penal corporativa de Leoncio Prado, 2017-2018
- Tellez, V. J. (2009). Derecho Informático. México: Mc Graw Hill. Obtenido de Editorial Mc Graw Hill.
- Vilca, A. G. (2018). Los Hackers: "Delito informático frente al código penal peruano". Obtenido de Repositorio de la Unkversidad Nacional Santiago Antúnez de Mayolo: http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2496/T033_47272593_T.pdf?sequence=1&isAllowed=y
- Zorrilla, T. K. (2018). Inconsistencias y ambigûedades en la ley de delitos informáticos Ley N. 30096 y su modificatoria Ley N. 30171, que imposibilitan su eficaz cumplimiento. Obtenido de Repositorio de la Universidad Santiago Antúnez de Mayolo: http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2332/T033_70221905_T.pdf?sequence=1&isAllowed=y