UNIVERSIDAD PERUANA DE LAS AMÉRICAS

ESCUELA PROFESIONAL DE DERECHO

TRABAJO DE INVESTIGACIÓN

LA EVIDENCIA DIGITAL Y SU INFLUENCIA EN LOS DELITOS INFORMÁTICOS EN LA CORTE SUPERIOR DE JUSTICIA DE AREQUIPA, 2019

PARA OPTAR EL TITULO PROFESIONAL DE ABOGADO

AUTOR:

ARANÍBAR SALAZAR MANUEL HUGO

CÓDIGO ORCID: 0000-0001-9573-459X

ASESOR:

MG. PANTIGOZO LOAIZA MARCO HERNÁN

CÓDIGO ORCID: 0000-0001-6616-0689

LÍNEA DE INVESTIGACIÓN: DERECHO PENAL, CIVIL Y CORPORATIVO

LIMA, PERÚ

DICIEMBRE, 2021

Resumen

El presente trabajo de investigación se llevó en el ámbito del Derecho Penal con la finalidad de conocer cuál era la situación actual de los Procesos Penales sobre el valor probatorio de la evidencia digital y su influencia en los delitos informáticos en la Corte Superior de Justicia de Arequipa, 2019, como la normativa a nivel nacional e internacional.

Debido a la existencia de una nueva Inseguridad Ciudadana, los Delitos Informáticos han aumentado notablemente, siendo la admisión del valor probatorio de la evidencia digital fundamental para la existencia de Juicios Justos. Es así, que las nuevas tecnologías han incrementado enormemente las probabilidades de resolver casos de delitos informáticos con la evidencia digital.

Asimismo, el desarrollo acelerado de las nuevas tecnologías ha impactado de manera preponderante las actividades que desarrollaban las personas a diario, creando una nueva dependencia al manejo de apps o aplicativos que facilitan la vida diaria, pero esto también facilita la vulneración de la intimidad de la persona, sus servicios, sus cosas, sus actividades. El mundo virtual es nuestro mundo real ahora y hay que dotarlo de seguridad. La necesidad que una evidencia digital sirva coma prueba digital fehaciente donde el tema central sea la admisión de esta dentro del proceso, con esto llegar a vincular el valor probatorio de la evidencia digital con la resolución de casos de delitos informáticos con el hecho delictivo y tenga un Proceso Penal correcto.

Palabras claves: Delitos Informáticos, Evidencia Digital, Derecho, Derecho Proceso Penal.

Abstract

The present research work was carried out in the field of Criminal Law in order to know what was the current situation of Criminal Proceedings on the probative value of digital evidence and its influence on the computer crimes, such as regulations at national and international level.

Due to the existence of a new Citizen Insecurity, Computer Crimes have increased notably, with the admission of the probative value of digital evidence being fundamental for the existence of Fair Trials. Thus, new technologies have greatly increased the chances of solving cybercrime cases with digital evidence.

Likewise, the accelerated development of new technologies has had a preponderant impact on the activities carried out by people on a daily basis, creating a new dependence on the management of apps or applications that facilitate daily life, but this also facilitates the violation of the privacy of the person, their services, their things, their activities. The virtual world is our real world now and it must be provided with security. The need for digital evidence to serve as reliable digital evidence where the central issue is the admission of it within the process, with this to link the probative value of digital evidence with the resolution of cases of computer crimes with the criminal act and have a correct Criminal Procedure.

Key words: Computer Crimes, Digital Evidence, Law, Criminal Procedure Law.

Tabla de Contenidos

Contenido

Resumen iii

Abstract iv

Tabla de Contenidos v

Introducción 1

Desarrollo del tema Bases teóricas 5

Conclusiones 37

Aporte de la investigación 39

Recomendaciones 41

Referencias bibliográficas 43

Introducción

Desde la aparición de la Internet, se han evidenciado muchos adelantos, pero a la vez ha permitido globalizar las oportunidades para llevarse a cabo delitos, llegando a puntos inimaginables del planeta tierra. Este comportamiento va en incremento muy rápidamente, convirtiéndose en un desafío tanto como para la policía y las autoridades judiciales de nuestro país y del planeta.

Frente a esta problemática se deben presentar nuevos desafíos y buscar la capacitación de las profesiones relacionados a este medio, no solo del Perú sino también a nivel mundial, en todas las áreas, en todas las profesiones, ya que es un problema globalizado.

La División de Delitos de Alta Tecnología de la PNP, son los responsables directamente que analizar esta problemática que luego conjuntamente con los fiscales y jueces, tratarán de resolverlos.

La cooperación internacional es un elemento de apoyo, donde se lleva a cabo la obtención y cruce real de información para obtener la situación real del tema. Todo caso toma tiempo de investigación, donde un perito informático autorizado, presenta un informe que es dirigido al Fiscal y luego al Juez.

Primero debemos entender que el sujeto que comete el delito no es un tipo común que se encuentra en la calle y comete un delito, sino el criminal está detrás de una computadora con una cadena de red, un servidor, que maneja dispositivos que se convierten en prueba. Que estas pruebas pueden ser auto alterables, o auto destructibles, programadas anticipadamente, Llegando a ser dispositivos volátiles. Es decir, el observador altera el objeto observado.

Este tipo de conducta indebida mayormente queda impune, debido a la falta de preparación y conocimiento de nuestras autoridades tanto judicial coma policial, las cuales les falta las herramientas y procedimientos correctos para investigar este tipo de delitos.

Es necesario implementar un procedimiento o un método adecuado para manejar investigaciones relacionadas con equipos informáticos, cumpliendo con la premisa de que estas prácticas deben ser aceptadas y puestas en acción de forma universal y respetando el debido proceso en el Proceso Penal Peruano.

Antecedentes nacionales e internacionales

Antecedentes nacionales

Herrera (2018) en su tesis para optar el título profesional de abogado, titulada: *“Eficacia de la ley de delitos informáticos en el distrito judicial de Huánuco 2017*”, tuvo como objetivo Demostrar el nivel de eficacia de la ley de los delitos informáticos en el Distrito Judicial de Huánuco 2017. La metodología aplicada fue de tipo básico, con un enfoque mixto, porque se utilizaron los enfoques cualitativo y cuantitativo, el nivel fue descriptivo simple; la población de estudio estuvo conformada por jueces y fiscales del distrito judicial de Huánuco, la muestra fue determinada por 30 personas, 15 jueves y 15 fiscales del distrito judicial de Huánuco, esta muestra fue no aleatoria, la técnica utilizada fue la encuesta y el fichaje y en instrumentos el cuestionario y fichas textuales y fichas bibliográficas. El autor llegó a la conclusión que la ley de delitos informáticos que se administra en el distrito judicial de Huánuco, tiene un nivel bajo de eficacia, esto a raíz de su imprecisión al regular las conductas infractoras.

Morales (2016) en su tesis para optar el título profesional de abogado, titulado: “*La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú 2025”,* en la facultad de Derecho, de la Universidad Señor de Sipán, tuvo como objetivo explicar la razón de ser de los delitos informáticos, como ha ido evolucionando hasta nuestros días, dar un acercamiento sobre la realidad que acontece en nuestro medio sobre la problemática que afecta a nuestra sociedad y la relación con el uso de la informática computacional como medio o fin, para la comisión de delitos, así mismo otorgar los elementos de información necesarios, para lograr una percepción social conveniente a fin de poder desarrollar una política de seguridad informática en nuestro medio. Dar una propuesta real de acción para el Legislador, con el fin que sus recursos humanos y materiales se aboquen al estudio, análisis y evaluación de esta problemática delictual, desarrollando los cursos necesarios para no ser sorprendidos y sobrepasados por esta nueva realidad nacional e internacional. Las técnicas utilizadas fueron: técnica del análisis documental y la técnica del cuestionario, la población está conformada por las normas y leyes peruanas relacionadas al tema. El autor concluye que la historia de la computación se remonta a los años 60s existiendo previamente a ello diversos aparatos rudimentarios que facilitaban las labores del ser humano como las calculadoras, instrumentos para realizar operaciones a través de tarjetas perforadas, inclusive hasta llegar al rudimentario ábaco, llegando hasta las computadoras que han sufrido diversas modificaciones a través de las denominadas "Generaciones", en las cuales han reflejado su avance y evolución que han ido teniendo durante cada 5 o 10 años, sin embargo, en la actualidad esos avances aparecen por cada año, inclusive mensualmente, ya que una computadora adquirida en una fecha, al mes siguiente es mejorada.

Antecedentes internacionales

Cortes (2014) en su monografía para optar el título de especialización en seguridad informática, titulada: "*Manejo de evidencia digital en dispositivos de almacenamiento pendrive USB aplicando la norma ISO/IEC27037:2012"*, presentado en la escuela de ciencias Básicas, tecnología e Ingeniería, de la Universidad Nacional Abierta y a Distancia, tuvo como objetivo Aplicar la norma ISO/IEC27037:2012 en el manejo de evidencia digital contenida en dispositivos de almacenamiento pendrive USB. La metodología de estudio fue exploratoria. El autor concluyó que Por medio del estudio de la Norma ISO/IEC 27037:2012 se identificaron lineamientos sobre los cuales fue viable incorporar procedimientos para el manejo de evidencia digital contenida en dispositivos de almacenamiento pendrive USB. Dichos procedimientos, aunque son ajenos a la ISO 27037, se plantearon de tal manera que permitieron explicar parte del contenido de la norma y adicionalmente se manejaron como texto de ayuda y a la norma y al lector que en un futuro decida comprobar su aplicabilidad en el campo de la práctica.

Lara, Martínez y Viollier (2014) en el artículo, titulado: *"Hacia una regulación de los delitos informáticos basada en la evidencia",* presentado en la Revista Chilena de Derecho y Tecnología, Centro de Estudios en Derecho Informático El estudio se basó en el análisis de la Ley 19223, del Gobierno Chileno y la información entregada por la Brigada de Investigación del Cibercrimen de la Policía de Investigaciones de Chile y por el Sistemade Asistencia a Fiscales del Ministerio Público. Otras solicitudes de información, dirigidas al Poder Judicial y al Ministerio de Justicia. Los autores concluyeron que la Ley 19.223 presenta una serie de deficiencias de redacción y aproximación jurídica a los fenómenos que pretende abordar, toda vez que no permite diferenciar o aplicar una pena proporcional según el nivel de afectación de la información o de la relevancia de esta última. El Convenio de Budapest representa lo más cercano a un modelo extranjero a seguir. En el ámbito de la tipificación de conductas, y atendidas las deficiencias de la legislación chilena, parece tomar fuerza la idea de la recepción de las normas sustantivas del Convenio; sin embargo, existen serios reparos a los aspectos procesales que hacen cuestionable la conveniencia de adherir a él. Conforme a la literatura, más allá de la adhesión al Convenio, es tarea del legislador adecuar la tipificación de figuras penales de manera sensata y acorde con los bienes jurídicos que se pretende proteger. Ya que un porcentaje cada vez mayor de nuestras interacciones se realiza en línea, la relevancia y participación de los delitos comunes cometidos por medios computacionales ha aumentado, y su tratamiento se ha transformado en un verdadero desafío para el derecho.

Desarrollo del tema Bases teóricas

Delito informático

El delito informático es una forma de exteriorización de las infinidades de conductas que el legislador consagra en el código penal como delito. Las heterogéneas actuaciones perjudiciales de ciertos agentes, han hecho que en nuestro país se vaya desarrollando esta rama del derecho penal. A diferencia de otros países como Estados Unidos, Australia, Francia, nuestro país no ha desarrollado a profundidad el tema. Este avance se ha dado por la necesidad de tener armas suficientemente eficaces para combatir los ataques y daños que por medio de los sistemas de cómputo se podían realizar a las personas o hasta la misma Nación.

En la actualidad encontramos diversas definiciones del concepto de delito informático, pero para hacer un acercamiento global de esta definición, podemos decir que es una conducta típica, antijurídica y culpable que realiza un sujeto agente utilizando técnicas informáticas para extraer o destruir información de personas naturales o jurídicas.

El delito informático se encuentra consagrado en la ley 30096 la cual se incluyó dentro del código penal, debido a las necesidades urgentes de reglamentar este tema materia de estudio. Sin dejar de lado la gran historia y la incidencia que ha tenido este tipo de conductas ya tipificadas en el mundo. Esta ley creo la protección de otro bien jurídico como lo es la información y los datos, de esta manera se podrán preservar íntegramente los sistemas que utilicen tecnologías de la información y de las comunicaciones, de igual forma tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se informen jurídicamente para evitar incurrir en alguno de estos tipos penales.

Fue necesario llegar hasta este punto debido a que nuestro análisis jurídico y material de la evidencia informática, está basado netamente en el delito informático, ahora la pregunta será la siguiente ¿Cuál es la importancia que tiene la prueba o la evidencia que se deriva de esos delitos informáticos? Y además de esto ¿será necesario que dicha prueba proveniente de un ilícito tenga que cumplir con ciertos requisitos procesales y sustanciales para que pueda ser valorado dentro de un proceso penal? Con esto nos referimos a si puede o no ser aceptada por el administrador de justicia.

La respuesta seguramente será afirmativa, si hacemos un comparativo con los requisitos que exigen la mayoría de las pruebas en cualquiera de las ramas del derecho. Podemos traer a colación una teoría que fue desarrollada por el catedrático italiano el señor Luigi Ferrajoli quien desarrollo la teoría general del garantismo penal, y que será nuestro punto departido para desarrollar los interrogantes anteriormente planteados. Ferrajoli dice que una constitución puede ser avanzadísima por los principios y los derechos que sanciona y, sin embargo, no pasar de ser un pedazo de papel si carece de técnicas coercitivas, es decir, de garantías que permitan el control y la neutralización del poder y del derecho ilegitimo, es por esto que el trata de hacer un análisis detenido de cómo el Estado protege efectivamente los derechos de los ciudadanos, ya que argumenta que la garantía de los derechos vitales de cada persona son condición indispensable para una convivencia pacífica.

Por lo anterior surge la necesidad no solo de que sean respetados todos los derechos que se han otorgado a través del tiempo a los ciudadanos, sino de que exista un ordenamiento jurídico completo tanto en el ámbito sustancial como en el ámbito procesal, de no existir este tipo de normatividades se daría lugar a que existieran lagunas jurídicas que traería como consecuencia la violación de derechos fundamentales otorgados a los seres humanos,llámese en un proceso penal el sujeto activo o el sujeto pasivo de u hecho punible. Laguna que posiblemente tuvo lugar con el nacimiento de un nuevo capítulo de la historia jurídica como lo son los delitos informáticos.

Teoría de la prueba

La noción de prueba aparece unida a todas las actividades de tipo social, puede afirmarse que es una necesidad que surge desde que el hombre vive en sociedad. En todas las ciencias reconstructivas, la prueba tiene una importancia fundamental, pues permite conocer el pasado, pero en el campo del derecho es vital para saber quien tiene la razón.

En el mundo del proceso civil como penal, la prueba es fundamental, esta se encuentra destinada a producirle certeza al juez, por lo tanto el reconstruye los hechos tal cual como se supone que ocurrieron y los subsume en la norma general y abstracta prevista por el legislador, para de esta forma darle aplicabilidad y concordancia con el caso en particular. Es necesario hablar de prueba judicial, para establecer un comparativo con la evidencia informática que se obtiene en este tipo de delitos, en este caso, la prueba va a recibir un tratamiento totalmente diferente a las pruebas que usualmente se utilizan en los demás procesos.

Prueba judicial

La prueba judicial es el acto o conjunto de actos destinados a la verificación científica (fáctica y reconstructiva) de la veracidad de los juicios jurídicos formulados sobre la ocurrencia de un delito y de su responsable, tiene un fin el cual es el de generar en el juzgador un convencimiento mas allá de toda duda razonable, sobre los presupuestos facticos de su decisión, cuyos artífices son el ministerio público, las partes e intervinientes en un proceso penal.

Para tener una noción de prueba penal lo más ajustada posible, es indispensable tener en cuenta las diferencias específicas, que, precisamente caracterizan las pruebas penales frente a las judiciales. Así en razón con sus elementos se destacan los siguientes de la clasificación que hace el profesor. Gustavo Cuello Iriarte (2008)

a) Su objeto esta constituido por los juicios jurídicos que, como resultado de la labor de investigación y en el cumplimiento de la función de acusar, formula la Fiscalía General de la Nación, al presentar la acusación ante el juez competente.

b) La actividad probatoria está a cargo de las partes e intervinientes (la Fiscalía General de la Nación, la defensa, la víctima y su abogado) y del ministerio publico. El juez es el director del proceso y por ende de la actividad probatoria, pero le está vedado decretar pruebas de oficio, en atención al sistema acusatorio con excepción de los jueces de control de garantías, "...empero, el juez de control de garantías, en aras de garantizar la eficacia de los derechos materia del control judicial, si puede decretar y practicar pruebas de oficio cuando lo considere indispensable".

c) Los medios de pruebas, que hacen parte de los medios de conocimiento son los establecidos en el Código Procesal Penal (prueba testimonial, prueba pericial, prueba documental y prueba de inspección) o cualquier otro medio técnico o científico que no viole el ordenamiento jurídico.

Principios de la prueba aplicados a los delitos informáticos

El profesor Jairo Parra Quijano, hace una enumeración interesante sobre los principios generales de la prueba que son los que les ayudan a los administradores de justicia a descubrir si verdaderamente el elemento material probatorio puede alcanzar la suficiente certeza para ser tenido en cuenta dentro de un proceso penal. En ellos encontramos:

1. Principio de la veracidad

Si en el proceso debe reconstruirse o hacerse una vivencia de cómo ocurrieron los hechos, para sobre ellos edificar la sentencia, las pruebas deben estar exentas de malicia, o falsedad. Cuando los testigos comparecen, a un proceso, están obligados a decir la verdad, a no deformarla.

2. Principio de la libre apreciación

La convicción del juez debe haberse formado libremente, teniendo en cuenta los hechos aportados al proceso por los medios probatorios y de acuerdo con las reglas de la sana critica, de ahí que cumplan todas las reglas establecidas en la ley, para que se pueda hablar de formación libre del convencimiento

3. Principio de la unidad de la prueba

Cuando se regla que el juez expondrá razonadamente el merito que le asigne a cada prueba, no cabe duda que se consagra el método analítico, el estudio individualizado de cada medio probatorio, las diferencias que se hacen y las reglas de la experiencia que se aplican. Este medio de prueba explicado en la sentencia muestra al justiciable y a la sociedad la manera ponderada y cuidadosa como el funcionario estudia las pruebas. Permite de igual forma observar que medio de prueba fue mal evaluado, para poder utilizar los recursos. La valoración conjunta viene después del estudio individualizado de cada medio o elemento probatorio.

“En materia penal el encartado tiene virtual y realmente a su favor la presunción de inocencia y ella obliga, en todo momento que se haga la valoración de la prueba a un estudio analítico de cada medio en particular y, una vez hecho, se razone sobre la influencia que cada una ejerce en la conclusión a que se ha llegado”.

4. Principio de igualdad

La oportunidad para conocer la investigación penal que se ha iniciado, debe ser inmediata, para los sujetos procesales. Si no se hace esa comunicación en el tiempo indicado se rompe la igualdad, y como sostiene Jaime Bernal Cuellar y Eduardo Montealegre: “mientras (el Estado) que ejerce la plenitud de su poder investigativo, el imputado no participa en la aducción de medios probatorios que posteriormente se pueden usar en su contra”.

Este principio tiende a lograr un equilibrio en el proceso, las partes tienen que tener igualdad de oportunidades para pedir y obtener que se les practiquen pruebas y para contradecir las del contrario, pero y sobre todo un conocimiento de los hechos, que interesan en general a la investigación.

5. Principio de la publicidad

La prueba puede y debe ser conocida por cualquier persona ya que, proyectada en el proceso, tiene un carácter social, hace posible el juzgamiento de la persona en una forma adecuada y segura. Es posible, cumpliendo este principio, que terceras personas puedan reconstruir los hechos.

6. Principio de la formalidad y legitimidad de la prueba

La prueba debe ser aprehendida, para el proceso en forma valida, requiere el cumplimiento de formalidades de tiempo, modo y lugar y, además, su inmaculación, exenta de vicios como error, fuerza o dolo.

En materia penal a diferencia que en el ámbito civil la prueba pese a que puede provenir de una autoridad competente como es la policía judicial, puede que no tenga valor probatorio alguno sino cumple con las exigencias establecidas en materia penal, como lo es cuando empieza la etapa de instrucción solo este cuerpo policial puede actuar si tiene orden expresa del fiscal, de no ser así esta prueba seria nula de pleno derecho y no se podría tener en cuenta en un proceso.

Es en este principio donde vale la pena anotar que dentro de las investigaciones que se adelantan en los delitos informáticos, la policía judicial llámese cualquier autoridad que sea competente para determinado caso, tiene que seguir los lineamientos existentes si los hay, de forma estricta, puesto que ellos son en primera instancia quienes tienen contacto directo con la prueba, por lo tanto, no pueden dejar de ninguna manera que la evidencia recolectada pueda ser viciada.

7. Principio de la libertad de los medios de prueba

En materia penal se ha afirmado que los medios de prueba deben estar taxativamente enumerados, por ello se ha dicho que las normas sobre las pruebas penales son normas de garantía, por lo cual toda su disciplina debería ser considerada como instrumento de defensa para el imputado. El medio de prueba, no es solamente un asunto procesal, sino también es una oportunidad de tutelar los derechos individuales constitucionalmente garantizados, frente al peligro de sus posibles violaciones.

8. Principio de la separación del investigador y del juzgador

En penal el Estado que es el más interesado en saber que fue lo que realmente ocurrió, no lo sabe y por ello tiene una doble misión: averiguar dónde está la información e informarse.

9. Principio delicitud de la prueba

La prueba ilícita es la que se obtiene violando los derechos fundamentales de las personas. La violación se puede haber causado para lograr la fuente de la prueba o el medio probatorio. A diferencia de la prueba ilegal, que es aquella que se obtuvo con violación del procedimiento penal establecido.

La licitud en materia informática, viene conexa a las diferentes actividades que realiza la policía judicial, no basta con que efectivamente se recolecte la prueba dentro de un lugar o en elementos informáticos en los cual se tenga orden judicial para inspeccionar, la actividad de búsqueda y recolección es mucho más técnica que recoger un pedazo de tela o acordonar un lugar, para obtener algún indicio que sirva de prueba.

Informática

Hoy en día se escucha mucho este término, pero ¿Que significa realmente la informática? Pues bien, según la RAE, es el "Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras". En otras palabras, " es el manejo de la información por medio automatizados"

Por otro lado, de acuerdo con Téllez Valdés, "La palabra informática es un neologismo derivado de los vocablos información y automatización, sugerido por Phillipe Dreyfus en 1962. En sentido general, podemos considerar que la informática es un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información con miras a una adecuada toma de decisiones".

Asimismo, Alberto Suarez Sánchez define la informática como "la técnica apoyada en la ingeniería de la información, que comprende el estudio y la sistematización del tratamiento de la información y sus diferentes formas de automatización". Así pues, en virtud de todo lo tratado hasta el momento, resulta lógico concluir que la informática es el tratamiento automatizado de la información.

Evidencia digital

Definición

Según Ghosh (2004) citado por (Cortés, 2014) la evidencia digital se define como "Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático" (p.22).

Menciona Casey (2003) citado por (Cortés, 2014) “la evidencia digital es un tipo de evidencia física construida por campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales” (p.22).

International Organization on Computer Evidence (IOCE)

Es un organismo internacional que involucra agencias gubernamentales que llevan a cabo investigaciones relacionadas a las evidencias digitales y plantea seis principios:

- Principio 1.- en el manejo de una evidencia digital, se deben aplicar los principios procedimentales y forenses generales.
- Principio 2.- cuando se obtenga evidencia digital no pueden ser cambiadas.
- Principio 3.- toda persona que manipule evidencia digital debe ser preparada anteriormente.
- Principio 4.- todas las acciones llevadas a cabo para obtener, conservar y trasladar evidencia digital deben estar completamente documentada, preservadas y disponibles para ser revisadas en cualquier momento.
- Principio 5.- el responsable del manejo de la evidencia digital es responsable en todo momento de ella.
- Principio 6.- todas las agencias gubernamentales que se relacionan con la obtención, acceso, conservación y traslado de la evidencia digital es responsable de cumplir con estos principios.

Características

La evidencia digital o electrónica es un conjunto de datos análogos como audios, videos, fotos u otros elementos que son digitales o pueden convertirse en digitalizables, aunque en su inicio no hayan sido. Para Sergi (2018) citado por (Del Valle, 2018) las características que presenta los datos informáticos o evidencia digital, fueron desarrollados por el Consejo de Europa y presenta las siguientes características:

La evidencia digital. - no es visible a simple vista solo para las personas con conocimientos y preparación técnica especial. La información que se encuentra almacenada en los dispositivos informáticos es útil para aquellas personas especializadas en este tema y la conservación de ella es también un tema delicado.

La evidencia digital es frágil y volátil. - puede en cualquier momento ocurrir que las evidencias no permanecen mucho tiempo en la red, de otro lado también puede ocurrir que al cambiar el estado original de la evidencia pueda alterar el contenido.

El contenido original puede ser alterado o destruido. - el estado de la memoria de los dispositivos electrónicos cambia sea por decisión del usuario o bien automáticamente, por el sistema operativo. En otras palabras, la evidencia digital, tiene un alto grado de ser alterada.

Masividad de la información digital. - cada año surge nuevos dispositivos electrónicos que poseen mayor capacidad de almacenamiento y los costos económicos cada vez menores.

La evidencia digital puede copiarse sin límites. - el contenido electrónico se puede copiar muchas veces y cada una de ellas son iguales al original.

Principios rectores de la evidencia digital

Según ISO/IEC 27037 (2012) la evidencia digital posee tres principios fundamentales:

La relevancia. - son elementos relacionados a la situación que se investiga, con la finalidad de probar una hipótesis que se planteó inicialmente. Aquellos elementos que no son relevantes serán excluidos.

La confiabilidad. - valida el proceso y deben ser auditables y repetibles para que los resultados sean iguales o similares.

Suficiencia. - las evidencias recolectadas y analizadas son elementos suficientes para sustentar los hallazgos y verificar las afirmaciones de la investigación.

Fuentes de la evidencia digital

La evidencia digital se encuentra en diferentes instrumentos o equipos relacionados a la tecnología, donde la información se envía a través de una red, las fuentes de evidencia digital pueden ser clasificadas en los siguientes grupos:

Sistema de computación abierta. - está relacionado a las computadoras personales y computadoras portátiles y los servidores.

Sistemas de comunicación. - está compuesto por las redes de telecomunicaciones, la comunicación inalámbrica e internet.

Sistemas convergentes de computación. - está formado por los teléfonos celulares inteligentes (smartphones) los asistentes personales digitales PDAs, las tarjetas inteligentes.

Aseguramiento de la escena del delito

El aseguramiento de la escena del delito será llevado a cabo por funcionarios de la Policía Judicial que cuenten con conocimiento técnico avanzado para el manejo de la evidencia digital, y dar cuenta rápidamente al Fiscal. La policía Nacional bajo la conducción del Fiscal podrá llevar a cabo las siguientes acciones:

Recoger y conservar los objetos e instrumentos referentes al delito.

Levantar planos, tomar fotos, realizar grabaciones y otros.

Efectuar un inventario de los secuestros e incautaciones necesarias en los casos de delitos flagrantes o de peligro inminente de su perpetración.

Luego, la investigación será conducida por el Ministerio Público, es importante asegurar que este proceso se lleve a cabo por personas calificadas en el tema, técnicos de experiencia para garantizar el éxito de esta etapa. Asegurar la escena del delito consiste en proteger y delimitar la escena para evitar la modificación o destrucción de las evidencias digitales. Las actividades realizadas fuera de los protocolos pueden modificar o alterar las evidencias.

Los investigadores que lleguen a la escena del delito deberán cumplir los siguientes recaudos:

Establecer los parámetros de la escena del delito. - las primeras personas en llegar a la escena deberán observar las características físicas del lugar, de igual manera todos los sistemas de información y de red que se encuentren,

Observación, valoración y planificación. - la planificación de las actividades antes de la llegada a la escena del delito será muy importante para el éxito de la recopilación de información. Se plantean escenarios principales y secundarios, se fijan prioridades y se asegura la seguridad de los especialistas. Revisar la existencia de sistemas integrados de videovigilancia, monitoreo de imágenes tanto dentro como fuera de la escena deberán ser registrados.

Delimitar la escena del delito. - demarcar el lugar de la escena del delito donde se encuentra la evidencia a recolectar, las vías de acceso y salida, zonas cercanas, vehículos o medios de transporte, etc. Se debe registrar estos espacios a través de fotos, videos, croquis y planos.

Asegurar la identificación de testigos, policías, médicos, bomberos, personal especializado

Establecer las medidas de seguridad. - asegurar todas las medidas necesarias para velar la seguridad de los investigadores y la escena.

Facilitar los primeros auxilios. - brindar los servicios médicos necesarios por parte del personal de emergencia para las víctimas del delito y para preservar las evidencias.

Asegurar físicamente la escena. - este momento es importante para asegurar la cadena de custodia de las evidencias, debiendo identificarlas y etiquetarlas de acuerdo a los principios y metodología apropiada.

Dónde encontrar la evidencia

La evidencia se puede encontrar en:

1.- Dispositivos de almacenamiento informático

Unidades de disco rígido internas: discos de aluminio o vidrio, recubiertos de material ferro magnético, cabeza de lectura/escritura.

Discos rígidos externos: requieren fuente de alimentación y un USB, FireWire, Ethernet, conexión inalámbrica.

Medios extraíbles: unidades de disco para almacenar, archivar y transportar datos.

Pendrive (USB): Dispositivo de almacenamiento extraíble mediante conexión USB.

Tarjeta de memoria: dispositivo de almacenamiento de datos de uso en cámaras digitales, teléfonos celulares, reproductores de música digital, notebook, consolas de videojuego, PDAs, Smart TV.

Posibles evidencias: mensajes de correo, historial de navegación de Internet, Chat de Internet, listas de registros, fotografías en distintos formatos de archivos (JPG, PNG, GIF, BMP, TIF), archivos de imágenes, documentos, archivos de texto, metadatos de archivos, claves en memoria, claves de encriptación, etc.

2. Dispositivos portátiles

Teléfonos celulares

Smartwatches

PDAs

Dispositivos digitales multimedia

Cámaras digitales

Sistemas de posicionamiento global (GPS)

Reproductores

Video filmadoras

Localizador

Sistemas en vehículos

Cámaras de seguridad

Posibles evidencias: Listado de llamados, mensajes recibidos y enviados, páginas de Internet visitadas, datos de localización geográfica, aplicaciones de software, documentos, mensajes de correo, historial de navegación de Internet, chat de Internet, fotografías, archivos de imágenes, base de datos y registros, mensajes de voz, redes Wi-Fi detectadas.

3. Dispositivos periféricos

Teclado

Mouse

Parlantes

Cámaras

Fax

Teléfonos

Router

Módem

Impresoras

Escáneres

Fotocopiadoras

Contestadores automáticos

Posibles evidencias: Entrada y salida de números de teléfonos y fax, llamados recientes, fax en la memoria, documentos impresos, impresiones dactilares, ADN, etc. Estos dispositivos pueden aportar evidencia física que permita vincular al usuario con el dispositivo digital incautado.

4. Redes de computadoras

Consta de dos o más computadoras conectadas por cables de datos o conexiones inalámbricas que comparten recursos e incluso de impresoras, periféricos, y dispositivos de enrutamiento de datos (*hubs, switches y routers*).

Posibles evidencias: Pruebas de software, documentos, fotos, archivos de imágenes, mensaje de correo y archivos adjuntos, base de datos, historial de navegación de Internet, registros de eventos y chat, datos almacenados en dispositivos externos.

Delitos informáticos

- **Definición**

Como señala Camacho (1987) citado por (Acurio, 2017) "En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia". (p. 7)

Acurio (2017) define que: "la 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 finalidad causar una lesión o poner en peligro un bien jurídico cualquiera”. (p.14)

En los últimos años se escucha diferentes términos relacionados a la tecnología y el crimen como delitos: computacionales, digitales, telemáticos, cibernéticos o fraudes informáticos. Uno de los países con mayor incidencia legal para combatir este tema es Estados Unidos, donde nace el concepto *cybercrime*, y a partir de ahí se hizo viral la preferencia del concepto “delito cibernético” así aparecen en los documentos de organismos internacionales como la ONU (2000,2010).

Actualmente por el incremento de las TICS en el mundo, aparecen nuevos ilícitos tipificados como delitos informáticos. Frente a este gran problema mundial, donde está relacionada la tecnología, se formularon leyes que puedan prevenir y combatir las diversas actividades ilícitas que dañan la credibilidad de la tecnología, el secreto de las comunicaciones y la estabilidad emocional, económica, social y política de los seres humanos. Las principales vulneraciones son: la falta d sistema de control en la red, aumento incontrolable de usuarios y la libertad de acceso a la tecnología, la incógnita identificación de usuarios en la red y la sencillez para acceder a la información.

Algunas acepciones

-Delito electrónico

Es muy frecuente encontrar este término para la denominación de este tipo de delitos, no obstante, es necesario remarcar que la expresión con la que comúnmente se utiliza es la siguiente: “delito informático o electrónico”, de modo que es utilizado indiferentemente de su significado al igualarse con la informática.

Técnicamente, la palabra electrónico como tal hace referencia a aquellos aparatos por los que pasa un circuito de electricidad de baja potencia. Por ello se habla obligatoriamente de un soporte físico para el cual no es necesaria la comunicación entre dos dispositivos. Sin embargo, al hablar de soporte electrónico se engloban muchos elementos, como un amplificador de sonido o una videoconsola, que nada tienen que ver con el delito que se trata en este trabajo. Por lo tanto, este término, desde el punto de vista técnico, queda rechazado.

-Delito informático

Éste es el término más utilizado para determinar este tipo de delitos tanto en la jurisprudencia española como en la legislación europea. En el primero de estos ejemplos, puede comprobarse al realizar una búsqueda en la base de datos que ofrece el Tribunal Supremo, en cuya búsqueda se ha incorporado un sistema de terminación de palabras en las que aparecen “delito informático grave” y “delito informático, cibernético” como los términos correctos por los que puede limitarse la búsqueda. En el segundo caso, si se hace una búsqueda en la legislación contenida en la web de la Comisión Europea podrá encontrarse, en la traducción castellana, sólo como tal el término de delito informático.

Así mismo, autores no pertenecientes a organismos del poder judicial también utilizan, en su gran mayoría, este término. Su utilización se lleva a cabo tanto en España como en el resto de Europa; algunos de los autores que lo utilizan son: Carlos Sarzana, tratadista penal italiano, Santiago Mir Puig, Catedrático de Derecho Penal en la Universidad de Barcelona, y Richard Mansfield, experto en seguridad informática, entre otros.

En un vocabulario específico el término informático se refiere a la informática, que es la ciencia aplicada que abarca el estudio y aplicación del tratamiento lógico y automático de la información. Por lo tanto, se entiende como cualquier medio para el procesamiento de la información, es decir, para dar una serie de órdenes. Esto incluye tanto los dispositivos que se utilizan (por ejemplo, el ordenador) como las acciones que se realizan dentro de éstos (por ejemplo, los programas de ordenador).

Los dispositivos físicos que abarca son prácticamente casi todos (debido a lo dicho anteriormente sobre que son cualquiera que procese información), esto engloba tanto los magnéticos como los digitales.

-Delito digital

Este término aparece escasamente en la bibliografía especializada. No obstante, es bastante utilizado en Argentina, esto puede comprobarse a través de sus periódicos (la mejor prueba sociológica del uso de un término) y del lenguaje utilizado por sus bufetes, como el de La Nación y Ernest & Young.

Dentro de un argot técnico digital se dice de la representación de información por medio de dígitos, refiriéndose por lo tanto al uso del sistema binario para la codificación de la información manipulada.

Este término se limita únicamente a aquellas máquinas que utilicen el sistema binario, dejando fuera a aquellas que no lo usan como, por ejemplo, la radio o el teléfono, que son analógicos. Sin embargo, al igual que ocurría con la electrónica, hoy en día casi todos los aparatos son digitales, por ejemplo, un lector de CDs o un reloj o una calculadora, y constituyen un mundo demasiado amplio y variado para el ámbito que nos compete.

-Delito telemático

Éste es un término relativamente utilizado en todo el mundo en su gran mayoría para determinar un delito realizado a través de un medio de comunicación. La mayoría de los organismos que lo utilizan incluyen, como una parte de ello, al delito informático.

El término telemático hace referencia a la telemática, que se refiere a todo lo relacionado con las técnicas y servicios relacionados con las telecomunicaciones. Es decir, constituye cualquier medio de comunicación. Al igual que se ha hablado anteriormente, éste es otro de los términos que es necesario rechazar debido a la amplitud de delitos que pueden llevarse a cabo a través de este tipo de medios sin referirse al área de este trabajo. Algunos de estos ejemplos son las estafas telefónicas, para las que se necesita un emisor real y físico y el teléfono como medio de comunicación, o la duplicación de la tarjeta de un teléfono móvil; para ninguna de éstas es necesaria la conexión a Internet.

-Cibercrimen

Ciber es una palabra comúnmente utilizada en países latinoamericanos parar referirse al mundo de Internet, y es allí donde puede llegar a aparecer en su bibliografía, al igual que el término electrónico. Una vez más varios términos pueden ser utilizados como si de uno se tratara para denominar el mismo concepto.

Gramaticalmente ciber es un prefijo utilizado para describir temas relacionados con Internet, por ejemplo: ciberespacio (término utilizado para referirse al universo virtual de datos que forma la red de Internet por el cual se puede navegar para consultar información), cibercafé o ciber lenguaje, entre otros. Y crimen es como se denomina a un delito grave.

Este término es impreciso por dos razones:

1. Al referirse ciber sólo a Internet se está delimitando a aquellas acciones que se realicen a través de éste, eliminando automáticamente la implicación de otras tecnologías informáticas para cuya utilización no es necesario Internet.

2. Crimen es un término demasiado específico, por lo que sería más apropiado utilizar delito en general.

Para la elección del término más apto será tenida en cuenta la adecuación técnica, la frecuencia de uso (que suele conllevar que sea un término más conocido), y la utilización en nuestro país o países cercanos. Atendiendo a estas características nos decidimos por "**delito informático**". Se ha escogido informático en lugar de los otros términos citados por las siguientes razones:

Frente a la electrónica. - debido a que ésta sólo abarca dispositivos electrónicos para los que no es estrictamente necesaria una comunicación, mientras que la informática, aunque no se requiere de una conexión a Internet a priori sí va ser necesaria para la comisión del delito.

Frente a digital. - ya que, como se ha dicho anteriormente, ésta sólo abarca dispositivos, como su propio nombre indica, digitales; sin embargo, la informática incluye tanto los digitales como los magnéticos.

Frente a la telemática. - porque ésta incluye todo tipo de medios de comunicación, mientras que la informática se limita a los que requieren de dispositivos informáticos.

Frente a ciber. - ya que éste sólo se refiere a acciones y al espacio virtual, mientras que la informática se refiere también a los dispositivos.

Características

Los delitos informáticos ofrecen infinidad de facilidades a la hora de su comisión debido a que reúnen una serie de particularidades específicas. Estas facilidades son las que caracterizan este tipo de delitos en comparación con los delitos en general.

Una de las características más destacada es la eliminación de la barrera del espacio ya que, debido a la utilización de la red de Internet que llega a cualquier lugar del mundo, no es necesario estar presente físicamente en el lugar donde se cometa el delito.

La supresión del factor tiempo también es una de las principales propiedades. Ésta supone una enorme ventaja para la comisión de los delitos debido a que no es necesario estar utilizando el ordenador en el mismo momento en que se lleva a cabo el delito. Un claro ejemplo de esto es el envío de virus y otros programas informáticos dañinos que pueden ser enviados a cuentas de correo electrónico y ser activados días, semana o meses después siendo entonces cuando el daño, y por lo tanto la acción delictiva, se produce.

Otras características que aportan este tipo de delitos es la alta probabilidad de que su comisión sea descubierta en un periodo de tiempo considerable después de que ésta haya sido llevada a cabo. A esto también ayuda el hecho de que, gracias a las nuevas tecnologías, la comisión del acto delictivo puede darse de una forma extremadamente rápida ya que, por ejemplo, el acceso a cuentas y datos personales puede llevarse a cabo saltándose una seguridad informática, que en muchos casos es mínima, y para la que se han creado programas de invasión específicos.

A esto se suma que, siendo sencilla y rápida (en ocasiones) la comisión del delito, éste pueda ser encubierto por la facilidad de realizar varias tareas al mismo tiempo en el mismo dispositivo de acceso.

Al contrario de lo que pueda pensarse, no se requiere una formación extremadamente especializada en informática para cometer este tipo de delitos, sino que existen multitud de acciones delictivas que pueden ser llevadas a cabo por cualquier persona que sepa realizar tareas básicas. Llama la atención como se pueden encontrar manuales que explican cómo desarrollar el p*hissing* o el *keylogger* y otros en la propia red, por lo que cada vez más los delitos están al alcance de cualquier persona con un perfil de usuario novel.

Evidentemente, aunque para las acciones más simples no haga falta experiencia informática y para las que conlleven un poco más de dificultad existan manuales, siempre va a haber un tipo de delito informático que sólo puede ser cometido por personas expertas en la materia. Éstos son los delitos de mayor envergadura como, por ejemplo, irrumpir en un sistema informático de las fuerzas de seguridad de un país.

Internet supone una red libre abierta a cualquier persona, para lo que, no es obligatorio tener una formación específica. No obstante, un dato significativo en la utilización de las nuevas tecnologías es la necesidad de adaptación por parte de las personas adultas y la falta de ella a los jóvenes que han nacido en la llamada era de la informática. Es por esta razón por la que, para estos jóvenes, en su gran mayoría menores de edad, es más sencilla la comisión de un delito informático.

El hecho de que Internet sea ya un elemento necesario en nuestra vida cotidiana y laboral facilita la comisión de delitos a través de terminales que no sean de uso doméstico y personal. Hoy en día casi todas las tareas de trabajo se realizan a través de la red, y prácticamente todos los centros públicos (ya sean educativos o lucrativos) y comercios privados (acudiendo a una publicidad fácil) ofrecen dispositivos de acceso. Por ello es posible la comisión de actos ilícitos en el lugar de trabajo y otros lugares públicos como bibliotecas o cibercafés.

Como ya se ha comentado, los delitos informáticos brindan una serie de ventajas a los autores de los mismos, esto conlleva que a su vez impongan inconvenientes a aquellas personas que intenten resolverlos.

El principal es la dificultad de su comprobación. Esto es debido a su carácter técnico, lo que dificulta el seguimiento de un rastro fiable, por lo que en ocasiones es casi imposible determinar quién es el autor y la terminal de origen. A ello se suma la complejidad a la hora de encontrar pruebas y mucho más de que éstas sean tomadas como evidencias judiciales.

Por si fuera poco, la tarea de resolver delitos se dificulta por la facilidad que tienen las nuevas tecnologías de borrar pruebas o de desviarlas y/o codificarlas por la red de forma que es casi imposible su identificación.

Son muchos los casos de delito informático (en cualquiera de sus niveles) y pocas las denuncias que se interponen. Ello es debido a la falta de una regularización legislativa y de medios pertinentes que dificulta la investigación de los casos. Todo esto desemboca en que tanto la investigación como la defensa de dichas causas suponga un coste económico elevado.

Categorías

La ONU ha establecido una serie de delitos informáticos de acuerdo a esta clasificación son:

El acceso no autorizado. - es el acceso a una red o sistema sin autorización,rompiendo los controles de seguridad del propietario, también se le conoce como *hacking*, para algunos autores este grupo no deberían afrontar un proceso penal porque son personas meramente curiosas, que solo revisan información personal, pero sin intención de conocer el contenido o realizar un acto ilícito. Otros ingresan a redes personales para incluir en ellas información ofensiva y perjudicial para los propietarios. Para la ONU este delito es difícil de probar porque necesita el testimonio de la víctima y el victimario; algunos países europeos, Sudáfrica y en algunos estados de EEUU han reglamentado este tema y prohibido algunos dispositivos para combatir la piratería informática como los *keyloggers* o programas de registro de actividad de teclado.

El daño a los datos o programas informáticos. -aquí ingresan a las redes de información y borran o dañan la información almacenada. Habitualmente se realiza a través de los llamados “gusanos” o virus informáticos, también se puede cometer un abuso a las fallas de seguridad de los programas.

El sabotaje informático. - consiste en la alteración, borrado o anulación de datos o programas, también se puede dar como interferencias en los sistemas informáticos con la finalidad de impedir el buen funcionamiento del sistema de computadoras o de telecomunicaciones.

La interceptación no autorizada. - consiste en la captación de información, sin la debida autorización, de comunicaciones que se originan en un sistema o red técnica.

El espionaje informático. - refleja la adquisición, revelación, transferencia o utilización de un secreto comercial sin la autorización de la persona natural o jurídica a quien le pertenece, con el objetivo de ocasionar una pérdida económica o aprovechar este conocimiento en beneficio de unos terceros, quienes no tienen derecho a ello.

Bases legales

Convenio de Budapest (2001)

Está compuesta de 48 artículos divididos en cuatro capítulos con sus respectivas secciones.

En el Perú, el 30 de enero del 2019, se aprobó la suscripción en el pleno del Congreso la incorporación del Perú al Convenio de Budapest que significa un gran avance y promueve la competitividad y el bienestar en un ambiente de confianza digital para las empresas y para todos los ciudadanos.

Legislación internacional

A nivel internacional, hay diferencias entre los países, tomando como eje el valor probatorio de los soportes informáticos; por ejemplo: EEUU., Gran Bretaña, Alemania y países nórdico, prevalece la libertad de prueba, los juzgadores valoran los medios de prueba, eficacia probatoria y como producirlos. A diferencia de Francia, Bélgica e Italia, donde prevalece la exigencia legal de la prueba escrita. Gran Bretaña, Australia, República Federal de Alemania, Austria, Suiza, Suecia y Francia dan la oportunidad a otro tipo de medios de prueba por los adelantos técnicos.

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 a la firma digital que la firma escrita en papel.

La ley de 1994 para las personas que realizan ataques de virus, presenta dos niveles para el tratamiento de quienes crean virus:

a) Para los que intencionalmente causen un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.

b) Para los que lo transmitan sólo de manera imprudencial, la sanción fluctúa entre una multa y un año de prisión. (Tellez, 2009)

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, estableció que el documento electrónico tenía el mismo valor probatorio que el documento en papel escrito, como estipula el artículo 1315 y 1316 (1, 2 y 3).

En España, en 1999, aplicaron un régimen específico a las relaciones telemáticas, y en el 2003 se publicó la ley de firma electrónica que coincide con el Real decreto ley y

Directiva comunitaria en que se basa. En el Nuevo Código Penal de España, el artículo 264-2, se aplicará la pena de prisión de uno a tres años y multa, a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos con una intensión dolosa, y cuando el hecho es cometido por funcionarios públicos se penaliza con inhabilitación. Con las estafas electrónicas, en el artículo 248, sólo tipifica las estafas con ánimo de lucro cuando el infractor se vale de alguna manipulación informática, pero no detalla las penas a aplicar en el caso de la comisión del delito.

En Alemania, en 1986 la Ley contra la Criminalidad Económica, se refiere a los siguientes delitos:

a) Espionaje de datos.

b) Fraude informático.

c) Alteración de datos.

d) Sabotaje informático.

En Austria, 1987, en el artículo 148 sanciona a aquellos que con dolo causen un juicio patrimonial a un tercero de tal manera que influyan en la elaboración de datos automática, mediante el diseño del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos.

En gran Bretaña, por a un caso de hacking en 1991, comenzó a regir la Computer Misuse Act (Ley de Abusos Informáticos). Con esta ley, el intento, se complete o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Aquellos que liberan un virus tienen penas desde un mes a cinco años.

En Holanda, en 1993 entró en vigor la Ley de Delitos Informáticos, donde se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría) y la distribución de virus. En el caso de virus sea con intención o sin intención, se penaliza de un mes en prisión si no fue con intención y hasta cuatro años si fue con intención.

En Francia, en 1988, dictó la ley relativa al fraude informático, que dicta penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión que suprima o modifique datos. La ley en su artículo 462-3 penaliza una conductaintencional para perjudicar a terceros que altera un sistema de procesamiento de datos. En el artículo 462-4 incluye en su tipo penal una conducta intencional y un tipo doloso y pena el mero acceso y agrava la pena si resulta la supresión o modificación de datos contenidos en el sistema, o la alteración del funcionamiento del sistema (sabotaje). En su artículo 462-2 tanto el acceso al sistema como que se mantenga en él, aumenta la pena, si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

En el Perú, la carta magna es la Constitución Política del Perú de 1993 en el Título I y V. En el código penal, el Título IV y V, menciona lo relacionado a Delitos Informáticos.

En la Ley N.27309, incorpora los Delitos informáticos al Código Penal, capítulo X.

Ley N. 30096, Capítulo II.

Decreto Legislativo N. 635, Capítulo X:

-Uso indebido de base de datos (Delito Informático) Artículo 207-A.

-Destrucción de base de datos. - (Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras) Artículo 207-B.

-Forma agravada. - (Delito informático agravado) Artículo 207- C.

En el código penal peruano:

a) Delito de Violación a la Intimidad.

b) Delito de Hurto agravado por Transferencia Electrónica de Fondos, telemática en general y empleo de claves secretas.

c) Delito de Falsificación de Documentos Informáticos.

En el Código Penal Peruano (C.P.), entre los delitos contra la fe pública, que son aplicables a la falsificación y adulteración de micro formas digitales tenemos los siguientes:

i) Falsificación de documentos.

ii) Falsedad ideológica.

iii) Omisión de declaración que debe constar en el documento.

iv) Delito de Fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos.

v) Delito contra los derechos de autor de software.

Esta ley fue muy cuestionada por todos los expertos, que debió volver a Comisión en el mejor de los casos, o pasar al archivo y volverse a plantear una propuesta de la adhesión del Perú al Convenio de Cibercrimen, en un marco de respeto irrestricto a las libertades y derechos constitucionalmente protegidos, y en dicho marco plantear una legislación en materia de delitos informáticos, analizar qué hacer con los delitos por medios informáticos y brindar herramientas de informática forense a la Policía. Luego la Ley N. 30171 modifica a la Ley N. 30096.

Artículo 1º Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10 Artículo 2º Acceso Ilícito (….)

Artículo 3º Atentado a la Integridad de Datos Informáticos (….) Artículo 4º Atentado a la Integridad de Sistemas Informáticos (….)

Artículo 5º Proposiciones a adolescentes, Niños y Niñas con fines Sexuales con fines a la Integridad de Datos Informáticos (….)

Derecho comparado

Países en los cuales se ha tenido que tipificar dichas conductas delictivas por cuanto las mismas violentan los derechos de los socios y usuarios y de la ciudadanía.

En Chile el 28 de mayo de 1993, se promulgó la ley 19.223 pero no fue hasta la fecha 7 de junio de 1993 que se publicó. Esta ley, tipifica y sanciona los denominados Delitos Informáticos.

Los delitos tipificados en la Ley 19.223 consideran como un bien jurídico la calidad, la pureza e idoneidad de la información que está contenida en cualquier sistema automatizado de tratamiento de la información. Además, no solo se protege el bien, sino que también los siguientes:

El patrimonio, en el caso de los fraudes informáticos.

La privacidad, intimidad y confidencialidad de los datos, en el caso de espionaje informático.

La seguridad y fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos probatorios mediante algún sistema o medio informático.

El derecho de propiedad sobre la información y sobre los elementos físicos y materiales de un sistema de información, en el caso de los delitos de daños.

Estados Unidos

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al

Acta de Fraude y Abuso Computacional de 1986.

En el mes de julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores.

Venezuela

Concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001.

La ley tipifica cinco clases de delitos:

Contra los sistemas que utilizan tecnologías de información: acceso indebido (Art.6); sabotaje o daño a sistemas (Art.7); favorecimientos culposos del sabotaje o daño. (Art. 8); acceso indebido o sabotaje a sistemas protegidos (Art. 9); posesión de equipos o prestación de servicios de sabotaje (Art. 10); espionaje informático (Art. 11); falsificación de documentos (Art. 12).

Contra la propiedad: hurto (Art. 13); fraude (Art. 14); obtención indebida de bienes o servicios (Art. 15); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (Art. 16); apropiación de tarjetas inteligentes o instrumentos análogos (Art. 17); provisión indebida de bienes o servicios (Art. 18); posesión de equipo para falsificaciones (Art. 19);

□ Contra la privacidad de las personas y de las comunicaciones: violación de la privacidad de la data o información de carácter personal (Art. 20); violación de la privacidad de las comunicaciones (Art. 21); revelación indebida de data o información de carácter personal (Art. 22);

Contra niños y adolescentes: difusión o exhibición de material pornográfico (Art. 23); exhibición pornográfica de niños o adolescentes (Art. 24);

Contra el orden económico: apropiación de propiedad intelectual (Art. 25); oferta engañosa (Art. 26).

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el título noveno capítulo I y II.

El artículo 167 VI del Código Penal Federal sanciona con prisión y multa al que intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería está regulada en la Ley Federal del Derecho de Autor en el Título IV, capítulo IV.

También existen leyes locales en el Código penal del Distrito Federal y el Código penal del estado de Sinaloa.

En España, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de noviembre en el BOE número 281, de 24 de noviembre de 1995. Éstos tienen la misma sanción que sus homólogos no informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio de 2007 (recurso Nº 2249/2006; resolución Nº 533/2007) que confirmó las penas de prisión para un caso de estafa electrónica (phishing).

El Estado uruguayo aprobó en el año 2007 la ley Nº 18.237 denominada expediente electrónico cuyo único artículo autoriza el uso de expediente electrónico, de documento electrónico, clave informática simple, firma electrónica, firma digital y domicilio electrónico constituido en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales. Se hace referencia a esta ley porque es evidente que será de amplio tratamiento para el caso de los delitos informáticos, puesto que las conductas que autoriza pueden ser objeto de un ciberdelito.

Recomendaciones para no ser víctimas

Cada vez son más las personas que prefieren realizar transacciones financieras vía internet.

Se concretan en tiempo real, son más rápidas, se evitan las largas colas. Sin embargo, si no tomamos ciertas medidas de seguridad, estas operaciones pueden traer consecuencias lamentables.

1. No introducir datos como claves y número de tarjetas desde una red pública (cibercafé, centros comerciales, etc.).
2. Actualizar el sistema operativo para no tener vulnerabilidades de seguridad.
3. Contar con una contraseña diferente para cada sitio (correo, cuentas bancarias, etc.).
4. Disponer de un software antivirus actualizado que tenga control de navegación en internet.
5. Cambiar de contraseñas cada cierto tiempo.
6. Comprobar que es una página segura (https).
7. No hacer clic en enlaces sospechosos o que se reciban por e-mail de fuentes que no sean de confianza.
8. Verificar la dirección de internet de la institución a la que se va a acceder y el certificado de seguridad.
9. Comprobar que es una página segura (https).
10. De ser posible, no ingresar desde el enlace y dirigirse a la página oficial.

11. No hacer clic en enlaces sospechosos o que se reciban por e-mail de fuentes que no sean de confianza.

Conclusiones

1. La concepción de delito informático no tiene un tratamiento pacífico, ni en la doctrina, ni en las diferentes legislaciones nacionales estudiadas; razón por la cual debe afirmarse que el presente tema aún carece de uniformidad en el mundo jurídico. Sin embargo, el presente autor se circunscribe en aquella tesis que considera que la esencia del delito informático es la afectación a un bien jurídico propio de la informática, lo cual se concreta en nuestra legislación. De aceptar la tesis contraria, casi cualquier delito podría ser informático dado que la mayoría de los bienes jurídicos tradicionales pueden ser afectados hoy en día a través de medios informáticos.

De igual forma, si llegare a considerase el crimen informático como aquel delito tradicional que se comete por medios informáticos, existirán conductas que, a pesar de afectar la informática, no podrán ser punibles por no violentar aún un bien jurídico tradicional; tal es el caso del tráfico de software malicioso o el de la suplantación de sitios web para capturar datos personales.

2. En la presente investigación se pudo establecer que la evidencia digital independientemente de la denominación legal que se le dé, llámese documento electrónico, mensaje de datos, entre otros; es un medio probatorio generalmente admitido por las legislaciones penales estudiadas, ya sea que se trate como una prueba documental, como un elemento material probatorio, o como un medio de prueba autónomo; por lo que su uso en juicio para aducir la veracidad o falsedad de las circunstancias atinentes a los hechos fácticos en debate o a la responsabilidad penal del acusado, es válido.

3. Dentro de nuestro régimen penal la evidencia digital tiene una doble naturaleza al poder ser considerada como un documento a la vez que como elemento material probatorio o evidencia física.

Ello dependerá de las condiciones en las que este elemento sea obtenido, de tal forma que si alguna de ellas coincide con las dispuestas en la norma adjetiva penal, el mensaje de datos o la evidencia digital será considerada como un elemento material probatorio, por lo que así será introducido al juicio penal.

La relevancia de lo anterior radica principalmente en la forma de autenticación de la evidencia digital, ya que cuando se introduce como una prueba documental su autenticación se regirá por lo prescrito en el Código Procesal Penal; mientras que, si se introduce como un elemento material probatorio o evidencia física, la forma en la que esta debe ser autenticada..

4. La evidencia digital, al igual que cualquier otra prueba, debe cumplir todos los requisitos para poder ser considerada como tal, es decir, ser conducente, pertinente y útil para el proceso; así como ser practicada en un juicio oral, público, contradictorio, concentrado y en presencia del juez. Cumplido todo lo anterior, esta podrá ser considerada como una prueba al interior del proceso penal y podrá ser objeto de valoración por parte del juez de conocimiento.

5. Nuestro ordenamiento jurídico cuenta con una legislación muy robusta respecto de los temas tratados en la presente investigación; pues como pudo determinar, otras legislaciones no regulan expresamente lo relativo a la evidencia digital, como sucede en los Estados Unidos o, no regulan de forma adecuada, en opinión de este autor, lo relativo al delito informático por errar en la concepción frente al bien jurídico que este afecta, tal y como ocurre en España.

Aporte de la investigación

El aporte de la investigación esta enfocado para mejorar nuestro sistema penal para que pueda ofrecer mayores posibilidades en el enfrentamiento y control de la criminalidad relacionada con la utilización de medios informáticos y otras tecnologías afines, resulta imperioso incorporar nuevas conductas de este tipo en el Código Penal, así como en otras disposiciones referidas a los delitos informáticos. Defendiendo mi hipótesis, tengo a bien comenzar determinando que los delitos informáticos tuvieron orígenes por los años 1957, en épocas de la segunda guerra mundial, cuando se trataba de buscar maneras de dejar indefensos a los contrincantes, saboteándoles los medios de comunicación que tenían, y usar estas debilidades para poder someterlos.

Desde ese entonces hasta el momento se ha visto un crecimiento extensivo de las tecnologías informáticas acompañadas con las maneras de fraudentar con las mismas. Dentro del ámbito jurídico, la deficiencia de herramientas, tanto técnicas como legales han hecho que este tipo de delitos en muchos de los casos se vean en la impunidad provocando el crecimiento de los índices de criminalidad deja en la indefensión a los ciudadanos.

Los Hackers a través de sus acciones afectan los bienes jurídicos sustanciales como: libertad, intimidad, patrimonio, privacidad, buen nombre, y honor; conductas que generan a futuro para estas personas otro tipo de comportamiento y actos delictivos como robo, hurto, trata de personas entre otras, circunstancias por las cuales el nivel de criminalidad aumenta a nivel internacional, razón por la cual se conoce como delitos transnacionales. Cabe hacer énfasis que los ciber-delincuentes, son personas de un nivel socioeconómico de medio hacia arriba, debido a que los niveles bajos no tienen la oportunidad de obtener con facilidad el uso de estas tecnologías, por este motivo se ha denominado este tipo como delito de cuello blanco; convirtiendo así a la Sociedad de la Información en vulnerable y un problema demasiado grande para todos los países de mundo.

El estudio de campo realizado permite advertir sobre la incidencia de la criminalidad nacida por medio de las tecnologías de la información y comunicación, las cuales se manifiestan a nivel global en especial nuestro país de manera expedida e impune, como también permiten verificar que la mayoría de las entrevistas están de acuerdo en que los Hackers inciden en la criminalidad del Estado y que tienen responsabilidad notoria entorno a los vertiginosos índices delincuenciales que se manifiestan en el medio nacional e internacional, llegando en forma unánime a la decisión de adoptar la creación de una política criminal que contribuya a la prevención, erradicación y sanción de estas conductas delictuales, por lo que. muchas veces se hace imposible llegar a probar y vlalorar una evidencia digital.

Por otro lado, para la adecuación o incorporación de nuevas conductas delictivas en lo referente a las TIC, es fundamental contar con una norma legal que esté sujeta a los derechos y garantías establecidos en la constitución, y el desarrollo de la Comunicación e Información sea en forma equitativa y responsable, para que puedan ser estos regulados, controlados y administrados de manera correcta. Es necesario introducir en el ordenamiento jurídico normas claras y precisas que permitan la adecuada administración, gestión y control de los recursos no renovables de las naciones, así como el otorgamiento de acreditaciones, la interconexión, ocupación y uso del dominio público o privado para la instalación de redes, existiendo un régimen que tenga competencia y jurisdicción para poder sancionar estos recursos, en concordancia con los derechos humanos, tratados, acuerdos internacionales que se refieran a este tema, ya que estos son de vital

importancia para el desarrollo de la sociedad de la información y del crecimiento económico y tecnológico de la misma.

Recomendaciones

1. Es necesaria la participación del Ministerio Público, pues es el órgano encargado de la persecución penal o bien entidad encargada de velar por el cumplimiento de las normas en materia de los hackers y para ello debe de crearse una unidad específica dentro de dicha entidad para el cumplimiento de la ley y persecución de los hechos ilícitos y capacitar a los integrantes de la misma.

2. Es indispensable la creación y cumplimiento de normas legales efectivas aplicables a la realidad peruana y de la necesidad de crear un cuerpo normativo específico o bien crear un apartado especial en el código penal que incluya el mayor número de delitos informáticos, con términos adecuados a la actualidad que vive los peruanos.

3. Se recomienda al Organismo Legislativo, un proyecto de ley y que tome conciencia de la necesidad del mismo, por el cual se pueda disminuir los delitos informáticos que surgen de las redes sociales, así como el control y la prevención de los mismos en Perú y de esta forma erradicarla con el tiempo, ya que dichas acciones, se ven reflejadas en la opinión que posee la sociedad internacional en nuestro país.

4. Perú es uno de los muchos países que se encuentra atrasado en lo que a la regulación de la tecnología respecta, siendo el uso de la misma como un medio comúnmente utilizado para la comisión de los delitos es por ello que es necesario la regulación de términos como internet, redes sociales, sitios de web ilegales, etc. Pues vivimos en un mundo tecnológico y

por ello Perú debe de apegarse a este nuevo mundo, para combatir de forma eficiente el ciber-crimen, que surge de las redes sociales.

5. Se requiere de la contratación de personal calificado en escenas de crímenes informáticos, que estos sean profesionales capaces de realizar una labor eficiente en escena y en laboratorio, así como que estos reciban capacitación constante para mantenerse a la vanguardia de la tecnología que día a día va en aumento y con nuevas expectativas universales.

Referencias bibliográficas

Acurio, D. P. (2017). *Derecho penal informático.* Obtenido de Pontificia universidad Católica del Ecuador: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Boitia, G. L., Carvajal, G. J., & Cerinza, R. J. (2019). *Un reto para la policía nacional hacia la lucha contra los delitos informáticos asociados con el Bitcoin.* Obtenido de Policía Nacional de Colombia: http://biblioteca.policia.edu.co:8080/bitstream/handle/123456789/1413/3133BOTIA.pdf?sequence=1&isAllowed=y

Cortes, d. l. (2014). *Manejo de evidencia digital en dispositiovs de almacenamiento pendrive USB aplicando la norma ISO/IEC27037:2012*. Obtenido de Repositorio de la Universidd Nacional Abierta y a distancia: https://repository.unad.edu.co/bitstream/handle/10596/2660/12752280.pdf?sequence=3&isAllowed=y

Del Valle, L. D. (2018). *Evidencia digital.* Obtenido de Universidad empresarial siglo 21.

Herrera, U. L. (2018). *Eficacia de la ley de delitos informáticos en el distrito judicial de Huánuco 2017.* Obtenido de Repositorio de la Universidad de Huánuco:

http://200.37.135.58/bitstream/handle/123456789/1058/HERRERA%20URSUA%2C%20Lesly%20Monica.pdf?sequence=1&isAllowed=y

Lara, J. C., Martínez, M., & Viollier, P. (2014). *Hacia una regulación de los delitos informáticos basada en la evidencia.* Obtenido de Revista chilena de Derecho y Tecnología: file:///C:/Users/Yuri%20Mart%C3%ADnez/Downloads/32222-1-109679-1-10-20140731%20(1).pdf

López, B. S. (2016). *Los delitos informáticos y la investigación fiscal en las entidades financieras cooperativas, del segmento uno de la economía popular y solidaria en el cantón Ambato, provincia de Turgurahua.* Obtenido de Repositorio de la Universidad .

Morales, D. D. (2016). *La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú 2025.* Obtenido de Repositorio de la Universidad Señor de Sipan: http://repositorio.uss.edu.pe/bitstream/handle/uss/3161/MORALES_DELGAD

Ochoa, A. P. (2018). *El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación.* Obtenido de Universidad de Cuenca.

Osco, E. M. (2019). *La adminsibilidad y el valor probatorio de la evidencia digital en el Sistema Jurídico Peruano 2018.* Obtenido de Repositorio de la Universidad César Vallejo: file:///C:/Users/Yuri%20Mart%C3%ADnez/Downloads/Osco_EMA.pdf

Pardo, V. A. (2018). *Tratamiento jurídico penal de los delitos informaáticos contra el patrimomio, Distrito Judicial de Lima, 2018.* Obtenido de Repositorio de la Universidad César Vallejo: http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

Ramirez, R. D., & Castro, S. E. (2018). *Análisis de laevidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia.* Obtenido de Repositorio de la Universidad Nacional Abierta y a Distancia.

Reina, M. K., & Ramirez, M. G. (2019). *Manejo que se le ha dado al delito informático jurisprudencialmente en Colombia en los últimos.* Obtenido de Repositorio de la Universidad Cooperativa d Colombia: https://repository.ucc.edu.co/bitstream/20.500.12494/13166/1/2019_manejo_delito_informatico.pdf