! Las anteriores acciones son penadas en el artículo 232 del Código Penal de Costa Rica en su inciso e). 7

Reforma al código penal de Costa Rica, No. 9048 del año 2012.

FEDERACIÓN IBEROAMERICANA DE ASOCIACIONES DE DERECHO E INFORMÁTICA.

¡Hacia el Nuevo Paradigma de la Justicia y el Derecho!

XVIII Congreso Iberoamericano de Derecho e Informática.

FIADI 2014 – SAN JOSÉ, COSTA RICA.

---------- . ---------

Mesa Temática: Legislación y Jurisprudencia Informática.

Título: OBSERVACIONES A LA CONCEPCION DE LOS DELITOS INFORMÁTICOS Y EL TRATAMIENTO DE LAS EVIDENCIAS DIGITALES EN EL PERÚ.

Autoría:

Katty A. Pérez Ordóñez ([§])

Juan Carlos Herrera Miranda ([**])

Pertenencia Institucional: Universidad Andina "Néstor Cáceres Velásquez" - Perú

Sumario: 1. Resumen. 2. Seguridad Informática. 3. Los Tipos Penales en la Ley de Delitos Informáticos 30096, Modificatoria Ley 30171. 4.

[§] Socióloga y Abog. Mag. en Derecho Civil. Dr. En Derecho. Docente de Pre y Post grado. Ponente FIADI XVI (Quito-Ecuador) FIADI XVII (Santa Cruz-Bolivia) Autora de Artículos y Ensayos de Investigación Vox Juris-ICAP-Puno. Rev. de Investigación UANCV.y otros.

[**] Ing. de Sistemas M.Sc. en Ing. de Sistemas. Candidato a Dr. Ex Decano Fac. Ing. Sistemas. Docente de Pre y Post grado UANCV. Jefe de la Of. de Servicios Académicos OSA-UANCV.

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Interlineado: 1,5 líneas

Tratamiento de las Evidencias Digitales. 5. Propuesta de Prácticas Científicas para la Gestión de los Delitos Informáticos. 6. Conclusiones. 7. Referencias Bibliográficas,

I. RESUMEN

El paradigma que sustenta el desarrollo de la legislación informática penal, así como los instrumentos y herramientas que concurren para valorar los delitos informáticos en el Perú, registran que junto al empoderamiento y expansión de la Era del conocimiento y las comunicaciones; en la misma medida de aquel preciado desarrollo, a nivel global y en todas las esferas de la vida económica, social, cultural y política, se proyecta el nocivo crecimiento de la cyber-delincuencia, muy a pesar de la dación de novísimas leyes para judicializar penalmente a quienes atentan contra la seguridad informática.

Sin embargo, se percibe el Problema que la construcción de un Derecho propiamente Informático, recién se está encaminando y las diferentes formas de valorar los Delitos informáticos, así como sus evidencias y rastros digitales, son judicializados (interpretados, razonados y procesados) como delitos comunes, mediante la injerencia de conceptos, categorías y procedimientos que datan del clásico lenguaje jurídico de los códigos civil y penal principalmente. Sin embargo, la incorrecta tipificación de aquellos delitos y que no son sometidos a un riguroso examen con las herramientas científicas que proporciona (por ejemplo) la informática forense, conlleva graves secuelas delictivas que se enquistan en las esferas de la impunidad y la inseguridad jurídica informática y penal.

Para enfrentar este problema, analizamos críticamente los artículos pertinentes de la "Ley de Delitos Informáticos" 30096, modificada por la Ley 30171, dada el (22-X-2013) que consolida y deroga el Capítulo X de Delitos Informáticos del Código Penal Peruano (D.L. 635). Dicha Ley, identifica los Delitos contra Datos y Sistemas Informáticos, Delitos Informáticos contra la Indemnidad y Libertad Sexuales, Delitos Informáticos contra la Intimidad y el Secreto de las Comunicaciones, Delitos Informáticos contra el Patrimonio y Delitos Informáticos contra la Fe Pública.

Como resultado de nuestro análisis, presentaremos una propuesta de práctica de investigación científica, para el uso alternativo de técnicas y herramientas informáticas y criminalísticas, para detectar, proteger, documentar, preservar, analizar, evaluar y valorar indicios probatorios de valor jurídico penal, con la finalidad de contribuir con la construcción del Derecho Informático, de mano con el Derecho y la Justicia, entrelazados con las tecnologías de la comunicación, para el elevamiento del nuevo paradigma que sirva para "abrir los caminos de la paz, la convivencia civilizada y el progreso humano por medio del Derecho y la Justicia"

PALABRAS CLAVE: Legislación Penal Informática, Valoracion de Delitos Informáticos, Seguridad Informática, Evidencias y Rastros Digitales.

ABSTRACT. The paradigm that supports the development of computer criminal law, as well as instruments and tools which contribute to value cybercrime in Peru, which together recorded empowerment and expansion of the Age of knowledge and communication; the same extent of that precious development globally and in all areas of economic, social, cultural and political life, the harmful growth of cyber-crime projects, in spite of the

enactment of the newest laws to prosecute criminally threaten to computer security.

However, the problem is perceived to building a proper Computer Law, is heading new and different ways of valuing Computer crimes and digital evidence and its traces are prosecuted (interpreted, processed and reasoned) as common crimes by the interference of concepts, categories and procedures dating from the classical legal language of mainly civil and criminal codes. However, the incorrect classification of crimes and those who are not subjected to rigorous scientific examination tools provided (for example) computer forensics, carries serious criminal consequences that fester in the areas of computer impunity and legal uncertainty and criminal. To address this problem, we critically analyze the relevant articles of the "Law of Computer Crimes" 30096, amended by Law 30171, given the (22-X-2013) which consolidates and repeals Computer Crime Chapter X of the Peruvian Penal Code (DL 635). The Act identifies the Crimes Data and Systems, Computer Crimes against Sexual Freedom and Indemnity, Computer Crimes Against Privacy and Secrecy of Communications, Computer Crimes against Property and Computer Crimes against Public Faith.

As a result of our analysis, we will present a proposal for scientific research practice, for the use of alternative techniques and criminology and computer tools to detect, protect, document, preserve, analyze, evaluate and assess probative evidence of criminal legal value, with order to contribute to the construction of Information Law, the labor law and justice, intertwined with communication technologies for the upliftment of the

new paradigm that serves to "open the ways of peace, coexistence and civilized progress human by the law and Justice "

KEY WORDS. Computer Criminal Law, Computer Crime Ranking, Computer Security, Digital Evidence and trails.

II. SEGURIDAD INFORMÁTICA

Las nuevas figuras jurídicas creadas para coordinar, planear y promover la seguridad informática en el Perú, surgen como respuesta al inusitado crecimiento de la inseguridad y la cyber-delincuencia. ISO-IEC17799 (que representa el Estándar Mundial de Seguridad Informática) recomienda el conocimiento tecnológico y criminalístico del tema, mediante la acreditación y desarrollo de estrategias de organización de la Seguridad Informática. El conocimiento tecnológico, recomienda dominar el manejo de redes, ordenadores, servidores, softwares, aplicaciones, amenazas y riesgos en la arquitectura de los ordenadores y la normatividad jurídica penal, así como en el aspecto criminalístico del Derecho Informático y la Informática Forense. El conjunto de estos conocimientos, acredita la gestión de peritajes judiciales para la seguridad informática, que son producto de la Investigación científica y la aplicación de herramientas y programas aptos para sostener evidencias digitales, para resguardar investigar y presentar las mismas como Evidencias de Prueba, valederas jurídica y electrónicamente.

La seguridad jurídica está basada en una serie de presupuestos desarrollados por la Doctrina del Derecho y se refiere a las acciones de búsqueda y acopio de información o elementos de prueba, que puedan armonizarse con las garantías y los derechos fundamentales, y con criterios

de eficacia y eficiencia en la investigación y persecución de la cyber-delincuencia. Bajo la valoración de los siguientes principios ([††]):

Legalidad o tipicidad, que demanda la existencia de una ley previa que autorice la medida limitativa o de injerencia del derecho.

Judicialidad o control judicial, por el cual, toda injerencia que implique restricción de un derecho fundamental, requiere de la decisión del juez.

Idoneidad, por cuyo principio, la medida o injerencia dispuesta debe ser cualitativa y cuantitativamente apta para lograr los fines de obtención o aseguramiento de determinada fuente de pruebas.

Necesidad, para la adopción de medios de investigación, como única forma de lograr la obtención de elementos o información útil para los fines de equidad en la justicia.

Proporcionalidad, que corresponde a la armonía que debe existir entre la intensidad de la afectación del delito y la necesidad de la investigación según la gravedad del caso.

Los principios que regentan la seguridad informática, se fundamentan en los principios periciales Informático Forenses que se consignan:

- Principio de entidad pericial: Consiste en que los medios e instrumentos informáticos que constituyen una parte de la criminalística, se integran con una metodología propia, que permite asegurar la detección, identificación, documentación, preservación y traslado de la evidencia obtenida, con técnicas e instrumentos propios e inéditos.

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Sangría: Primera línea: 0 cm, Interlineado: 1,5 líneas

[††] DARAHUGE, María Elena y ARELLANO GONZALES Luis E. (2008) "La Prueba Indiciaria Informático Forense" SANS Institute, EUA.

- Principio de Protección y Preservación: Que requiere de una cadena de custodia estricta y con certificación unívoca comprobable.

- Principio de identidad de copias del original: Cuya valoración responde a que son identificables unívocamente.

- Principio Tecnológico interdisciplinario, según el cual, se requieren conocimientos específicos por parte de todas las ciencias involucradas en la prueba indiciaria.

- Principio de Compatibilización Legislativa Internacional. Mediante comunicaciones electrónicas, instrumentos en correo electrónico abierto o cerrado y certificado por medio de claves criptográficas o firma digital.

- Principio de Vinculación Estricta, por el cual las pruebas indiciarias deben estar relacionadas con la legislación Internacional, para resguardarse de los delitos de espionaje industrial, comercial, macro-terrorismo, pornografía infantil, trata de personas, blanqueo de capitales y genocidio.

Sin embargo, el problema de la tipicidad penal de los delitos informáticos, resulta demasiado complejo, dado que para un procedimiento de identificación-clasificación, es necesario en primer lugar, la concurrencia de otras disciplinas conexas, como la criminología, la criminalística, la medicina legal y para la configuración legal de la Prueba indiciaria, la fotografía, videos y otros rastros periciales que define la informática forense. Y en segundo lugar, es necesario la aplicación de los métodos internacionales establecidos para la certificación pericial, (los mismos no están claramente establecidos), por lo que en muchos casos, los jueces se inclinan por entender los delitos informáticos "como una forma novedosa de juzgar delitos tradicionales" porque aún es insuficiente el hecho de interpretar el leguaje técnico en los términos de un abogado y

Con formato: Fuente: (Predeterminada) +Cuerpo (Calibri), 14 pto, Sin Cursiva, Color de fuente: Automático

Con formato: Interlineado: 1,5 líneas

viceversa. Por otra parte, las complejidades técnicas, frecuentemente sobrepasan los conocimientos y la experiencia de los operadores judiciales, incluso algunos elementos de la evidencia digital pueden parecer intangibles, dada su naturaleza virtual o sus confusas similitudes con otros elementos de evidencia. Aquí es donde se presenta el problema de la adecuación de ciertas categorías de los "delitos comunes" del Código Penal a la Ley Informática, Este fenómeno puede deberse al hecho que hasta la actualidad, en el País no existe ningún Programa Académico-Profesional, ni carrera Técnica para capacitar en informática forense y/o peritaje informático, salvo aquellas entidades policiales que califican personal en crímenes de alta tecnología y son quienes ocupan el lugar de los informático-forenses, y por lo mismo, son los que están más ligados a la seguridad informática penal.

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: (Predeterminada) +Cuerpo (Calibri), 14 pto, Español (Costa Rica)

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

III: LOS TIPOS PENALES EN LA LEY DE DELITOS INFORMÁTICOS 30096.– Modificatoria 30171.

El (Art. 2) de la Ley de Delitos Informáticos, sobre el Acceso Ilícito, demanda: "El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de las medidas de seguridad establecida para impedirlo, será reprimido con pena privativa de libertad no menor de uno de mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado".

Este artículo, en primer término, tiene connotaciones que se derivan del intrusismo, categoría que hace referencia a la realización de operaciones contrarias al Numeral 10 del Artículo 2 de la Constitución

Política del Estado Peruano, que establece el Derecho a la Inviolabilidad de las Comunicaciones y Documentos Privados. "Reconociendo de este modo a la persona, la facultad de exclusión de la injerencia de extraños en sus relaciones privadas. En este sentido la protección del individuo, abarca todo tipo de intrusiones, sea cual fuere el ámbito en el que se produzca" (‡‡).

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Sin embargo, al referirse a todo tipo de intrusión de las comunicaciones, (que pueden ser epistolares, telegráficas, telefónicas, radiales, televisivas y de otras formas electrónicas de transmisión de mensajes o comunicaciones como el correo electrónico, internet, etc.) No precisa si esos accesos ilícitos o intrusiones pueden constituirse o no en formas de secuestro o incautación, aperturas, lecturas, interferencias o apropiaciones ilícitas dispuestas por una autoridad, administradores o cyber-delincuentes, por lo que se debe prever que la afectación al derecho a la Inviolabilidad de las comunicaciones, puede tener un carácter subsidiario, porque por comunicación se entiende, cualquier forma de transmisión del contenido del pensamiento, o de una forma objetiva de éste por cualquier medio. Además Karin Vigo (§§) sostiene que "La crítica más seria contra la Ley, apunta a que la norma es inconstitucional… porque restringiría la libertad de prensa y la libertad de expresión. Se ha tildado a la norma de Ley Mordaza, pues se afirma que busca penar a los medios de comunicación que publiquen información que haya sido obtenida mediante la interceptación telefónica o informática. Se ha dicho también, que la

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

‡‡ GALVEZ VILLEGAS, Tomás Aladino y otros (2009) "El Código Procesal Penal: Comentarios descriptivos, explicativos y críticos" D'JUS INSTITUTE Derecho y Justicia, Juristas Editores, Lima.

§§ VIGO, Karin. (2013) "Delitos Informáticos, Mitos y Verdades de la Novísima Legislación" Revista Jurídica

tipificación de algunos delitos es tan vaga que puede permitir a jueces y fiscales, considerar casi cualquier acción como delictiva, porque otorga el mismo tratamiento al medio por el cual se trasmite la comunicación, entendiendo por medio al soporte material o energético en el cual se porta o se trasmite la comunicación"

A propósito del control de las comunicaciones y documentos privados, Gálvez Villegas (***) comenta que: "La ley Nº 28950 en actual vigencia en nuestro medio, considera que solo es posible afectar el derecho de inviolabilidad de las comunicaciones y documentos privados, mediante interceptaciones y controles por parte de la autoridad competente, en casos de investigaciones de delitos graves tales como: secuestro agravado, trata de personas, pornografía infantil, robo agravado, extorsión agravada, tráfico ilícito de drogas, tráfico ilícito de inmigrantes, delitos contra la humanidad, atentados contra la seguridad nacional y traición a la Patria, peculado, corrupción de funcionarios, terrorismo y delitos tributarios y aduaneros; la Ley no establece nada al respecto, en cuanto se refiere a la interceptación, incautación y apertura de correspondencia"

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Otro de los problemas que gravitan en torno a la inseguridad informática y a los impedimentos del tránsito del clásico expediente escrito al expediente virtual, es el problema del uso de la misma gramática jurídica, adjudicada indistintamente para la judicialización de delitos comunes y delitos informáticos, estos últimos, deberían de merecer otro adecuado examen en cuanto se refiere a la Sintaxis Jurídica, la misma que presenta

*** GALVEZ VILLEGAS, Tomás Aladino y otros (2009) "El Código Procesal Penal": Comentarios descriptivos, explicativos y críticos" D'JUS INSTITUTE Derecho y Justicia, Juristas Editores, Lima.

serios problemas lingüístico-gramaticales al momento de la interpretación, tipificación, razonamiento y argumentación jurídica, "Pues, la característica fundamental del razonamiento jurídico es la capacidad de deducción de los enunciados relativos a las acciones humanas a partir de datos que incluyen normas de comportamiento, mientras que la sintaxis revela la relación de los signos lingüísticos entre sí, es muy precisa pero no dice nada del mundo, en cambio, la semántica se ocupa de la relación que tienen los signos con el mundo y esto es mucho más complicado, pues no existe una relación biunívoca entre palabras y objetos " ([†††])

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Es el caso concreto del presente análisis, que ha detectado problemas de SINONIMIA JURIDICA en la referida ley, que presenta una misma idea jurídica expresada a través de dos o más conceptos (palabras) muchas veces diferentes. Así, el concepto DAÑO del Art.3 "Atentado a la Integridad de Datos Informáticos" demanda: "El que deliberada o ilegalmente daña, Introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con …" Estos mismos conceptos (parecidos, sinónimos o semejantes) rezan en los Arts. 4 y 8 de la referida Ley. (Art. 4) "Atentado a la Integridad de Sistemas Informáticos" El que deliberada o ilegalmente inutiliza total o parcialmente un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios será reprimido con …" (Art.8) "Fraude Informático" reza: "El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de un tercero, mediante el diseño, introducción, alteración, borrado, supresión, clonación

[†††] MARTINO, Antonio (2013) "Lógica Informática, Derecho y Estado" Fondo Editorial Tiempos Nuevos, Universidad Inca Garcilazo de la Vega, Lima.

de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema, será reprimido con …"

De igual o similar forma los Arts. 2, 6, 7, 9 y 10, reiteran: "El que deliberada e ilegítimamente accede a un sistema, con vulneración de medidas de seguridad … (Art.2) "El que ingresa o utiliza indebidamente una base de datos … (Art.6) "El que mediante las tecnologías suplanta la identidad de una persona natural o jurídica … (art 7) "El que deliberada e ilegítimamente intercepta datos … (Art.9) "El que fabrica, diseña … u obtiene para su utilización … (Art.10) ¿No son sinónimos de INTRUSIÓN el que accede ilegítimamente, el que ingresa indebidamente o el que ilegítimamente intercepta datos? Ahora bien, el art. 8 repite: "El que procura un ilícito mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos, será reprimido… " El Art 10 vuelve a reproducir los términos "El que fabrica, diseña, desarrolla, vende ,facilita, distribuye, importa u obtiene …" Frente a dichas sinonimias, consideramos que el problema radica en la falta de visión y creatividad lingüística por parte del legislador, para poder diferenciar, clasificar y sistematizar los contenidos de las diferentes acepciones significantes, significativas, valorativas y típicas, con propiedades unívocas para la debida interpretación y tipificación de los fenómenos y hechos virtuales al interior de los delitos informáticos, los mismos que al parecer pudieran tener una misma connotación que los daños y los delitos comunes que configura el clásico Derecho penal. Tras esta disyuntiva, para los jueces y fiscales ¿Prima la valoración y concepción del daño físicamente probado?. ¿Y los daños virtuales? ¿Serán realmente virtuales o reales? Dicho problema

¿Constituye acaso, el eterno retorno hacia la irresoluta contradicción entre lo ideal y lo real o entre la real idealidad y la irrealidad?

También es el caso de las POLISEMIAS y analogías insertas en la Ley de Delitos Informáticos, que "novedosa" y reiteradamente involucra conceptos que contienen dos o más sentidos: "Impide el acceso, entorpece, interfiere, intercepta, altera, inutiliza, deteriora" ¿Son análogas, diferentes o semejantes, en alternancia virtual contra datos, sistemas, servicios o contra el Patrimonio?

Inexplicablemente, aparecen en esta instancia, varias analogías cuando estos mismos conceptos, se refieren a ideas parecidas que son usadas para apreciar, interpretar y documentar de modo clásico los rastros y evidencias virtuales recurriendo a las herramientas de la "Equivalencia funcional probatoria" equivalencia que subyace en el problema de la no distinción entre el valor de las "clásicas" pruebas documentadas y el valor de las "modernas" pruebas digitales, Las mismas que deberían contener conceptos, categorías y procedimientos jurídicos adecuados, fruto de la recopilación, búsqueda, acceso, almacenamiento y transferencia de evidencias y pruebas procesadas electrónicamente.

Caso similar sucede con la Integridad de Datos Informáticos del Art.3 y el Fraude Informático del Art 8 de la Ley, que relaciona los mismos términos: "El que a través de las tecnologías de la información o de la comunicación daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos Informáticos, y el Fraude Informático del Art 8 … el que inutiliza, impide el acceso, entorpece, imposibilita, intercepta, suprime, clona, etc." A estas alturas, el problema ya no constituye la complejidad de los crímenes de alta tecnología, ni la ausencia del dominio de las

herramientas tecnológicas y criminalísticas para recurrir a las alternativas periciales de la Informática forense; simplemente sucede la vulgarización repetitiva de conceptos entrecruzados en casi todos los artículos. De allí emerge la confrontación entre una prueba que puede tomar diferentes formas susceptibles de modificación, manipulación o desistimiento, por considerar aspectos y características similares a las pruebas afines "no obstante ello, resulta necesario afinar la redacción de algunos artículos (según lo expuesto), a fin de brindar seguridad jurídica. El objetivo sería lograr que la ley sea efectiva, respecto al principio de legalidad y criterios de proporcionalidad, evitando los tipos penales de peligro abstracto, así como las dualidades donde se establecen agravantes por el solo uso de la Tecnología, lo cual puede terminar minando un importante espacio de innovación como es el entorno digital" (‡‡‡)

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

IV.- TRATAMIENTO DE EVIDENCIAS DIGITALES.

Ahora bien, el Código Penal Peruano (CPP. DL. 635) en el Título V sobre Delitos contra el Patrimonio, sostiene que "el HURTO supone la existencia de un patrimonio que constituye el conjunto de bienes (muebles, inmuebles, dinero, valores, etc.) Considera como variantes del delito contra el Patrimonio, el hurto, el robo, la apropiación ilícita, el fraude, la estafa, la receptación, la extorsión, la usurpación y los daños". En este acápite, equipara como bien mueble a "la energía eléctrica, el gas, el agua y cualquier otra energía o elemento que tenga valor económico así como el espectro electromagnético" (6ª Edición, Colec. Jus INKARRI) Espectro electrónico que se tipifica como Bien Jurídico penalmente protegido,

‡‡‡ YouTube-IDEJUS-Lima-2014. "Ley de Delitos Informáticos en cuatro conclusiones".

cuando prima el concepto tradicional de ROBO configurado por el uso de la violencia y amenaza con peligro inminente para la vida y la integridad. Pero, un robo informático ¿Involucra necesariamente el uso de la violencia contra la integridad personal? Si así fuera el caso, el Juez, según la jerarquía de las leyes ¿Aplicaría la Ley de Delitos Informáticos o el Código Penal? Aun cuando la evidencia pericial, acogería la tipificación de bien mueble sustraído del lugar empleando violencia. Esta interrogante, conlleva en sí misma, una contradicción sobre la valoración de una evidencia caracterizada por su virtualidad.

En otro acápite, el concepto apropiación ilícita, que el propio Código Penal define como "recepción de un bien con asentimiento y negativa de devolución", apoya la conclusión, que no es recomendable el uso indistinto del lenguaje documentado para los casos virtuales, o para procesar casos de la misma naturaleza, en todo caso, el examen de las pruebas electrónicas deberá ser sometido a las características especiales que demandan las evidencias digitales, y son las siguientes: ([§§§])

"La Evidencia digital se puede reproducir y alterar fácilmente,

La Evidencia digital es anónima. En muchas ocasiones establecer la verdadera procedencia de un mensaje de datos no firmado digitalmente (por ejemplo) es muy difícil para alguien sin el debido entrenamiento.

La forma de la evidencia digital es tan importante como su contenido. Es importante revisar el contenido del documento.

La evidencia digital tiene dificultades para ser llevada a la corte.

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

[§§§] CANO MARTÍNEZ, Jeimy J. (2010) "El Peritaje Informático y la Evidencia Digital en Colombia, Conceptos, Retos y Propuestas" Ed. UNIANDES, Bogotá.

La recopilación, búsqueda, acceso, almacenamiento y transferencia de evidencia digital son tareas que exigen consideraciones y cuidados especiales para garantizar la integridad de ésta y la observancia de la cadena de custodia".

La admisibilidad y valoración de la evidencia digital, requiere de la confidencialidad, integridad, autenticidad, originalidad e inalterabilidad.

V.- PROPUESTA DE PRÁCTICA CIENTÍFICA PARA LA GESTIÓN DE EVIDENCIAS DIGITALES.

Con el uso creciente de las tecnologías de la información y las comunicaciones, las entidades, instituciones y organizaciones empresariales estatales y privadas, puedan innovar sus procesos y mejorar sus procedimientos administrativos, frente a los delitos informáticos y sus competidores, produciendo gran cantidad de información, para mejorar alternativamente sus métodos de gestión y trabajo.

Esto trae como consecuencia, que personas ajenas a dichas entidades y organizaciones empresariales, no puedan realizar operaciones y actos dolosos usando la informática, o causando ataques en contra de los sistemas informáticos (que generan grandes pérdidas económicas) y debilitan el empoderamiento del paradigma del Derecho y la Justicia. Para evitar aquellas contingencias, se desarrollan permanentemente, herramientas informáticas que permiten identificar a los intrusos y las formas de comisión de sus delitos, asegurando la obtención de medios probatorios, mediante el logro de evidencias digitales que serán utilizadas en un proceso judicial.

Una de estas herramientas es la Informática Forense, aun no sociabilizada en su totalidad sobre todo en nuestro país, es por esto que su implementación y utilización en un proceso judicial, puede ser cuestionado por desconocimiento absoluto o parcial, para evitar este hecho, la obtención de pruebas indiciarias, debe ser manejada en base a rígidos principios científicos, procedimientos y normas legales. Pues, su aplicación proporciona la resolución de actos delictivos informáticos, con apoyo del método científico, aplicado para la recolección, análisis y validación de todo tipo de pruebas digitales.

Para tipificar estos delitos informáticos, no solamente se hace referencia a la definición del procedimiento que deberá seguir un investigador al llegar a la escena del delito. Se trata de brindar a los jueces y fiscales elementos de convicción que deben tomar en consideración, cuando un perito especializado les presente evidencia de naturaleza digital, de modo que les permita decidir y resolver un caso, estableciendo un fallo, que depende del nivel de confianza y certeza que alcancen, al observar si esa prueba ha sido modificada de alguna forma, en algún momento. El procedimiento forense digital, busca precisamente, evitar esas modificaciones o distorsiones de los datos contenidos en el medio o dispositivo magnético a analizar, para que se puedan presentar en cualquier instante, desde el mismo momento en el que haya ocurrido el presunto hecho punible, como consecuencia del simple transcurso del tiempo, o el apagado fortuito o intencional del equipo.

Según el FBI, la informática (o computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

Con formato: Fuente de párrafo predeter., Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

La informática forense, en consecuencia, sirve para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital. Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional. Dentro de lo forense encontramos varias definiciones:

Computación forense (computer forensics): Disciplina de las ciencias forenses, que procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Forensia en redes (network forensics): Es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Forensia digital (digital forensics): Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos

Con formato: Fuente: +Cuerpo (Calibri), 14 pto, Español (Costa Rica)

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones.

Una evidencia digital es una información almacenada en un formato digital que puede llegar a ser utilizada como medio probatorio en un proceso judicial, para que esta pueda ser viable será necesario seguir un procedimiento para su recuperación, almacenamiento y análisis, es importante seguir una cadena de custodia robusta que permita asegurar la inmutabilidad de la evidencia digital.

Fases de un análisis forense digital. : (****)

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Identificación del incidente.- En esta etapa debemos buscar y descubrir las señales de un ataque a un dispositivo informático actuando en forma metódica y profesional asegurando que el procedimiento a seguir no de resultados distintos al fin. Para esto lo primero que se debe realizar es conservar la evidencia intacta y de ser el caso que se ha perdido parte de la información aun así se puede identificar indicios en dispositivos que hayan estado conectados al equipo. Para esta finalidad de identificación se utiliza verificaciones integrales informáticos usando utilidades de software.

Recopilación de la evidencia.- Para esta fase se debe establecer el método que permita identificar su origen, duración; extremando precauciones, tomando muestras sobre el sistema vivo o muerto.

Preservación de la evidencia.- Al obtener la recolección de evidencias se debe asegurar conservando intacta la información siguiendo procedimientos que mantengan su integridad y cadena de custodia.

Análisis de la evidencia.- En esta fase se aplica técnicas científicas y analíticas.

**** LOPEZ DELGADO, Miguel. (2007) "Análisis Forense Digital" Ed. CRIPTORED. Bs.As.

Documentación del incidente.- Se realizan reportes, informes en un leguaje que permita ser interpretado por los abogados y jueces, es decir es la elaboración de documentación que será presentada en un proceso judicial, entregando una información cuidadosa para mantener un prestigio técnico. Para dar soporte al proceso en estudio, que permita la tipificación de un delito informático a los jueces y fiscales, así mismo se brinde la obtención de medios probatorios y convicción de estos; existen herramientas informáticas como las que proponemos a continuación

Herramienta Forense EnCase:

Figura 1: Interfaz Encase Forensic

EnCase([††††]) es una grandísima herramienta utilizada para la informática forense. Es la más utilizada y líder en el mercado para esta utilidad. Sus características más importantes son:

Copiado Comprimido de Discos Fuentes: Permite crear copias comprimidas de los discos origen usando un estándar sin pérdida (loss-less). Los archivos comprimidos que obtendremos como resultados pueden ser buscados, analizados, y verificados de la misma manera que los archivos originales.

[††††] http://www.encase.co.za/support/index.shtm

.

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Justificado, Interlineado: 1,5 líneas

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Interlineado: 1,5 líneas

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Esta técnica nos ahorra mucho tiempo permitiendo mantener varios casos ya que podemos trabajar en paralelo y ahorrar espacio en el HDD donde estemos analizando las pruebas.

Búsqueda y Análisis de Múltiples partes de archivos adquiridos: Esto permite al informático buscar y analizar varias partes de la evidencia. Muchos investigadores utilizan varios discos duros, discos extraíbles, etc. Esta utilidad nos permite buscar todos los datos involucrados en un caso en un mismo paso. Estos datos se clasifican, si está comprimida o no, y podemos colocarla en un HDD y examinarla en paralelo. En varios casos, la información valiosa puede ser ensamblada en un hdd, servidor de red...

Diferente Capacidad de Almacenamiento: Los datos pueden ser colocados en diferentes unidades como HDD IDE, SATA, SCSI, ZIP y JAZZ. Los archivos que pertenecen a la evidencia pueden ser comprimidos o guardados en CD-ROM manteniendo su integridad forense intacta, pudiendo ser estos mismos archivos utilizados desde el mismo CD-ROM.

Varios Campos de Ordenamiento, Incluyendo Estampillas de tiempo: Esto permite ordenar los archivos de acuerdo a diferentes campos incluyendo las tres estampillas de tiempo (cuando se creó, último acceso, última escritura), nombres de los archivos, firma de los archivos y extensiones.

Análisis Compuesto del Documento: Permite recuperar archivos internos y meta-datos con la opción de montar directorios como un sistema virtual para la visualización de la estructura de estos directorios y sus archivos, incluyendo el slack interno y los datos del espacio unallocated.

Búsqueda Automática y Análisis de archivos de tipo ZIP y Attachments de E-Mail.

Firmas de archivos, Identificación y Análisis: La mayoría de las gráficas y de los archivos de texto comunes contiene una pequeña cantidad de bytes en el comienzo del sector los cuales constituyen una firma del archivo. Podemos verificar esta firma para cada archivo con una lista de firmas conocidas con extensiones de archivos. Si un sospechoso ha escondido un archivo o lo ha renombrado, detectaremos automáticamente la identidad del archivo.

Análisis Electrónico Del Rastro De Intervención: Herramientas para documentar y reparar información como Sellos de fecha, de hora, registro de accesos, etc.

Soporte de Múltiples Sistemas de Archivo: Reconstruye los sistemas de archivos forenses en DOS, Windows (todas las versiones), Macintosh (MFS,HFS,HFS+), Linux (Sun, Open BSD), CD-ROM y los sistemas de archivos DVD-R.

Vista de archivos y otros datos en el espacio Unallocated: Provee de una interfaz similar al explorador de Windows y una vista del HDD de origen, también permite ver los archivos borrados y todos los datos en el espacio Unallocated. También muestra el *Slack File* con un color rojo, permitiendo saber cuando fue creado cualquier archivo que sobreescribió ese espacio.

Integración de Reportes: Realiza un análisis y una búsqueda de resultados, en donde se muestra los comentarios del investigador, imágenes recuperadas, favoritos, criterios de búsqueda, etc.

Visualizador Integrado de imágenes con Galería: Nos permite una vista completamente integrada que localiza automáticamente , extrae y despliega muchos archivos como .gif y .jpg del disco. Seleccionando "Vista

de Galería" se despliegan muchos formatos de imágenes, incluyendo las imágenes que han sido eliminadas.

Herramienta Forense WinHex: Software para informática forense y recuperación de archivos, Editor Hexadecimal de Archivos, Discos y RAM

Tener todos los bits de su ordenador al alcance de la mano se ha convertido en una realidad. WinHex(‡‡‡‡) es un editor hexadecimal universal, y al mismo tiempo posiblemente la más potente utilidad de sistema jamás creada. Apropiado para informática forense, recuperación de archivos, peritaje informático, procesamiento de datos de bajo nivel y seguridad informática. Sus características incluyen:

- Editor de disco por FAT12/16/32, exFAT, NTFS, Ext2/3/4, Next3®, CDFS, UDF
- Built-in interpretation of RAID systems and dynamic disks Various data recovery techniques
- Editor de RAM, una manera de editar RAM y la memoria virtual de otros procesos
- Intérprete de Datos que reconoce hasta 20 tipos distintos de datos
- Edición de estructuras de datos mediante plantillas
- Concatenar, partir, unir, analizar y comparar archivos
- Funciones de búsqueda y reemplazo especialmente flexibles
- Clonado de discos, con licencia especialista támbien sobre DOS
- Imágenes y backups de discos (comprimibles o divisibles en archivos de 650 MB)
- Programming interface (API) y scripts

‡‡‡‡ http://www.x-ways.net/winhex/index-e.html

- Encriptación AES de 256 bits, checksums, CRC32, digests (MD5, SHA-1, ...)
- Borrado irreversible de datos confidenciales/privados
- Importación de todos los formatos de portapapeles
- Formatos de conversión: Binario, Hex ASCII, Intel Hex y MotorolaS
- Juego de caracteres: ANSI ASCII, IBM ASCII, EBCDIC
- Salto instantáneo entre ventanas
- Documentación exhaustiva.
- Otras que podemos mencionas son:
- Sleuth Kit (Forensics Kit)
- Py-Flag (Forensics Browser)
- Autopsy (Forensics Browser for Sleuth Kit)
- Dumpzilla (Forensics Browser: Firefox, Iceweasel and Seamonkey)
- dcfldd (DDImagingTool command line tool and also works with AIR)
- foremost (Data Carver command line tool)
- Air (Forensics Imaging GUI)
- md5deep (MD5 Hashing Program)
- netcat (Command Line)
- cryptcat (Command Line)
- NTFS-Tools
- Hetman software (Recuperador de datos borrados por los criminales)
- qtparted (GUI Partitioning Tool)
- regviewer (Windows Registry)
- Viewer
- X-Ways WinTrace
- X-Ways WinHex

- X-Ways Forensics
- R-Studio Emergency (Bootable Recovery media Maker)
- R-Studio Network Edtion
- R-Studio RS Agent
- Net resident
- Faces
- Encase
- Snort
- Helix
- NetFlow
- Deep Freeze
- hiren´s boot
- Canaima 3.1
- Mini XP

En este capítulo se ha descrito los procedimientos que proporciona a la ciencia forense en materia de informática para la resolución de casos llevados a procesos judiciales con el objetivo de brindar y aportar al sistema jurídico herramientas especializadas, de tal manera que su utilización dependerá de la experiencia del investigador o perito.

Con formato: Interlineado: 1,5 líneas

VI.- CONCLUSIONES

PRIMERA.- Los tipos penales tradicionales resultan ambiguos e inadecuados para merituar y valorar las nuevas formas de los delitos informáticos, por cuanto las indicadas pruebas indiciarias, no cumplen con los requisitos, los principios y el estándar de valoración mundial, establecidos para la tipificación de los delitos informáticos del presente.

SEGUNDA.- Es necesario sopesar y re-elaborar los elementos tradicionales de la doctrina general de la prueba, así como el lenguaje jurídico que fue creado para cumplir funciones específicas en el tratamiento de los delitos comunes, los mismos que hasta la actualidad son utilizados para tipificar erróneamente los delitos informáticos. De ésta forma se puede contribuir con el empoderamiento del paradigma del Derecho y la Justicia, para abrir los caminos de la paz, la convivencia civilizada y el progreso humano.

TERCERA.- La actualización de los conocimientos, habilidades, destrezas y aptitudes, respecto del tratamiento de la cyber-delincuencia, deberá considerar una nueva lectura de los delitos por manipulación informática, en términos de interceptación, incautación, apertura de comunicaciones y datos; fraude por manipulación e introducción de datos falsos; cambios en los sistemas, soportes, programas y archivos; introducción de instrucciones para no realizar funciones no autorizadas; adopción de medidas de seguridad contra la falsificación de datos, delitos de espionaje industrial y comercial y el robo como privación de bienes electrónicos, la autoproducción de información contenida en redes, soportes y sistemas informáticos, etc.

CUARTA.- Es urgente la capacitación y formación de peritos informáticos, mediante diplomados, programas de segunda especialización y maestrías para profesionales del área de administración, contadores y auditores, abogados, jueces y fiscales, Ing. de sistemas, Ing. electrónicos, médicos forenses, antropólogos forenses, policía judicial y demás profesionales especializados en investigación informática penal. Cuyo perfil como Expertos en Evidencias Digitales les permita laborar como auxiliares de

justicia y asesores judiciales de entidades empresariales, privadas y estatales, así como investigadores y docencia superior.

QUINTA.- La admisibilidad de las pruebas electrónicas ante la justicia y el derecho, debe estar supeditada a la calidad, recolección y custodia, análisis científico y exhibición de pruebas. Por lo que, el modelo básico de enseñanza del peritaje informático en el Perú, deberá seguir los lineamientos de ACPO, tomando en consideración el Procedimiento Forense Estandarizado en sus cuatro etapas de Recolección, que implica la búsqueda, reconocimiento y documentación de la evidencia electrónica; Proceso de examen de la evidencia, para explicar su origen y alcances, contenido y estado de la evidencia en su integridad; Fase de análisis e inspección, indagando el valor probatorio y su relevancia; y el Reporte o declaración, mediante copia fidedigna de los datos objeto de investigación. Así mismo, el soporte teórico deberá incluir conocimientos sobre Derecho penal informático, metodología de investigación jurídica informática, criminalística y prácticas de laboratorio, entre otros.

SEXTA.- La informática forense es una herramienta indispensable que toda organización debe contemplar dentro de su política de seguridad y debe estar enmarcada dentro del proceso de respuesta a incidentes en los sistemas informáticos.

VII.- REFERENCIAS BIBLIOGRAFICAS.

1.- ALVAREZ DUEÑAS, Pedro. (2009) "Notificación Electrónica en el Poder Judicial" Editorial ADRUS, Lima.

2.- CANO MARTINEZ, Jeimy José. (2010) "El Peritaje Informático y la Evidencia Digital en Colombia, Conceptos, Retos y Propuestas" Ediciones UNIANDES, Bogotá.

3.- CORREA, Carlos M. (1994) "Derecho Informático" Ediciones DEPALMA, Buenos Aires.

4.- DARAHUGE, María Elena. (2008) "La Prueba Indiciaria Informático Forense" darahuge@yahoo.com.ar.

5.- GALVEZ VIILEGAS, Tomás Aladino. (2009) "El Código Procesal Penal, Comentarios Descriptivos, Explicativos y Críticos" Djus Jurista Editores, Lima.

6.- GIL ALBARRAN, Guillermo. (2007) "Derecho Informático" Grupo Editorial Megabyte, Lima.

7.- LOPEZ DELGADO, Miguel. (2007) "Análisis Forense Digital" Ed. CRIPTORED. Bs.As.

8.- MARTINO, Antonio A. (2010) "Lógica Informática, Derecho y Estado" Fondo Editorial Nuevos Tiempos UIGV, Lima.

9.- SALAZAR LLUEN, Daniel. (2009) "Perfiles Profesionales Para Seguridad Informática, Un Enfoque Práctico" Escuela de Ing. de Sistemas USS, Chiclayo.

10.- TELLEZ VALDEZ, Julio. (2013) "Lex Cloud Computing" Estudio Jurídico del Cómputo en la Nube en Mexico, IDIEJ-UNAM, México.

11.- VIGO, Karin (2013) "Derecho Informático, Mitos y Verdades de la Novísima Legislación" Jurista Editores, Lima.

12. YouTube-IDEJUS. (2014) "Los Delitos Informáticos en Cuatro Conclusiones"

Con formato: Fuente de párrafo predeter., Fuente: (Predeterminada) +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

- "Ley de Delitos Informáticos" Diario El Peruano, Normas Legales (22-X-2013)

- "Código Penal" (1998) Col.Jur INCARI, Lima.

- " Nuevo Código Procesal Penal" (2006) Jurista Editores, Lima.

- "Tecnología de Información. Código de Buenas Prácticas para la Gestión de Seguridad de la Información" NTP-ISO/IEC 17799:2004.

- "Sistema de Gestión de Seguridad de Información" NTP-ISO/IEC27001:2005. www.shellsec.net

- "La Seguridad Total" http://members.xoom.com/segutot/la.htm

-"La Seguridad Informática en Redes" www.geocities.com/SiliconValley/Bit/7123/la.htm

-"Auditoría de Tecnologías de Información" www.udi.edu/page.asp?page=sisteseguridad

-"Ingeniero de Seguridad Informática" www.zanajobs.com.ar/trabajo=452532-asp

- Lina Ma. Gorrón "Informática Jurídica Documental" COD.2009179630

- http://www.encase.co.za/support/index.shtm

- http://www.x-ways.net/winhex/index-e.html

Con formato: Fuente de párrafo predeter., Fuente: (Predeterminada) +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente de párrafo predeter., Fuente: (Predeterminada) +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente de párrafo predeter., Fuente: (Predeterminada) +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente de párrafo predeter., Fuente: (Predeterminada) +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Fuente de párrafo predeter., Fuente: (Predeterminada) +Cuerpo (Calibri), 14 pto

Con formato: Fuente: +Cuerpo (Calibri), 14 pto

Con formato: Justificado, Interlineado: 1,5 líneas