Modelo para el Análisis y Gestión de Riesgos en Fases carentes de Técnicas y Herramientas: Caso Tratamiento de la Evidencia Digital en el Entorno del software libre utilizando procesos unificados

Cruz Vela Erika Marilyn
Postgrado en Informática
Universidad Mayor de San Andrés - UMSA
La Paz, Bolivia
cruz.marilyn@gmail.com

***Resumen*— La razón fundamental del presente documento es el de presentar aspectos relacionados con los riesgos en el proceso de la recolección de evidencia digital en el entorno del software libre; para esto se realizarán consideraciones de la NIST y trabajos realizados en el área de la informática forense para proponer un modelo para la recolección de información en el entorno del software libre; como aspectos complementarios se realizará un análisis de los sujetos del delito informático, con un análisis de la situación internacional, situación nacional, casos nacionales, estadísticas en casos nacionales; para finalmente elaborar las conclusiones respectivas del documento.**

I. INTRODUCCIÓN

Durante los últimos años se detectaron una serie de problemas en el tratamiento de la evidencia digital, pero se puede detectar un problema central el cual viene expresado en la siguiente pregunta: ¿Cuáles son los riesgos en el tratamiento de evidencia digital cuando se utilizan procesos unificados de recuperación de información digital en software libre?

Para responder a esta problemática se plantea el siguiente objetivo: Considerando las recomendaciones de NIST (National Institute of Standars and Technology) y los trabajos realizados en el área de la informática forense, proponer un modelo para realizar el análisis en el proceso de recolección de la evidencia digital en software libre, de modo exista la gestión de riesgos en la recuperación de la información digital y de esta forma se puedan establecer informes claros en contra de acciones antijurídicas.

Para ello se pretende demostrar la siguiente hipótesis: el análisis y la gestión de riesgos en el tratamiento de la evidencia digital debe tratarse con un modelo razonable para que no fracture los procesos unificados en la recuperación de información digital, de modo que la evidencia digital es válida si se cumple con un modelo que cumpla con condiciones determinadas por recomendaciones internacionales; cumpliendo con este modelo la evidencia digital es considerada como un medio probatorio en un juicio.

Por lo tanto en el presente trabajo se pretende proponer un modelo para el análisis y la gestión de riesgos en el proceso de recolección de evidencia digital en el entorno del software libre, de modo que exista una metodología en la recuperación de información digital.

El análisis y la gestión de riesgos en el tratamiento de la evidencia digital debe tratarse con un modelo razonable para que no fracture los procesos unificados en la recuperación de información digital, de modo que la evidencia digital sea válida si se cumple con un modelo que cumpla con condiciones determinadas por recomendaciones internacionales; cumpliendo con este modelo la evidencia digital será considerada como un medio probatorio en un juicio.

En el presente documento se pretende investigar el delito informático que visto desde cualquier perspectiva es una tarea compleja. Las dificultades que surgen al tratar de aplicar el método científico a la delincuencia transnacional y al crimen organizado es la tarea a la que se ve abocado el Ministerio Público por mandato constitucional y por disposición legal. Ahora bien el fenómeno descrito en los últimos tiempos ha tenido un avance significativo tomando en cuenta la manifestación de la globalización, la cual no solo ha tenido beneficios, sino también ha contribuido a la masificación de esta clase de delitos y tecnificado a otra clase de cómo son los llamados delitos informáticos.

La realidad boliviana no es la excepción en el tratamiento de los delitos informáticos, el código penal como la constitución política del estado no estipula con claridad el análisis de este tipo de problemáticas.

Esta dependencia de la sociedad de la información a las nuevas tecnologías de la información y de las comunicaciones (TIC), hace patente el grave daño que los

llamados delitos informáticos o la delincuencia informática pueden causar a nuestro nuevo estilo de vida, la importancia que cobra la seguridad con la que han de contar los equipos informáticos y las redes telemáticas con el fin de poner obstáculos y luchar con dichas conductas delictivas, y la necesidad de tipificar y reformar determinadas conductas, a fin de que esta sean efectiva y positivamente perseguidas y castigadas en el ámbito penal.

Nuestro país en este sentido no puede quedar exento en este tipo de temas, debe empezar a tomar todas las acciones, medidas necesarias y prepararse para el futuro y así no quedar al margen de situaciones que podrían en forma definitiva terminar con la sociedad de la información boliviana, en este sentido el presente trabajo pretende ser un aporte a la escasa o inexistente doctrina, que en el campo del derecho penal que existe en nuestro país con respecto a la evidencia digital y a los llamados delitos informáticos en entornos del software libre.

II. Antecedentes De La Informática Forense

En 1970, los crímenes electrónicos iban en aumento, sobre todo en el sector financiero. La mayoría de los ordenadores de esta época fueron los mainframes, utilizados por personas capacitadas con conocimientos especializados que trabajaban en las finanzas, la ingeniería, y la academia.

A comienzo de los años 90, el FBI (Federal Bureau of Investigation) observó que las pruebas o evidencias digitales tenían el potencial de convertirse en un elemento de prueba tan poderoso para la lucha contra la delincuencia, como lo era el de la identificación por ADN. Para ello, mantuvo reuniones en su ámbito, y a finales de los años 90 se creó la IOCE (International Organization of Computer Evidence) con la intención de compartir información sobre las prácticas de informática forense en todo el mundo.

Posteriormente la Scientific Working Group on Digital Evidence (SWGDE), principal portavoz de la IOCE en Estados Unidos, y la Association of Chief Police Officers (ACPO) del Reino Unido, propusieron una serie de puntos que luego englobaron los principios generales que se presentaron en el año 2000 al Grupo de Lyón.

En la actualidad de acuerdo con la ISO/IEC 27037:2012 la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital, bien ésta sea utilizada para que sea admisible en corte o no.

En la actualidad quienes se dedican al análisis forense y la investigación digital conocen bien las mejores prácticas basadas en documentos publicados por el NIST (National Institute of Standars and Technology), el departamento de Justicia de los Estados Unidos y el FBI (*Federal Bureau of Investigation*) entre otros pero hasta el momento no existía una norma de alcance global como la ISO/IEC 27037 Guía para la Identificación, recolección, adquisición y preservación de evidencia digital, proveniente del tronco de normativa de Seguridad Informática ISO 27000.

III. Marco Teórico: Informática Forense, Evidencia Digital, Procesos Unificados, Delitos Informáticos

En el presente documento involucraremos teoría que está relacionada con la informática forense, evidencia digital, procesos unificados y delitos informáticos, por lo tanto en las siguientes líneas se comenzarán a desglosar cada una de ellas.

Comencemos a mencionar que la informática forense se define como una rama de la informática que se encarga de recolectar y/o recopilar información valiosa desde sistemas informáticos (redes, ordenadores, soportes magnéticos, ópticos, etc.) con distintos fines, sirviendo de apoyo a otras disciplinas o actividades, como son las labores de criminalística e investigaciones.

Se reconoce a Dan Farner y Wietese Venema, como los pioneros de la informática forense, actualmente Brian Carrier es probablemente uno de los expertos en el tema.

Esta disciplina está asociada a dos interpretaciones:

- Disciplina asociada con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso.

- Disciplina científica especializada en elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Estas dos interpretaciones son complementarias, la una hace énfasis en las consideraciones informáticas y la otra en la especialidad técnica, ambas procuran el esclarecimiento e interpretación de la información en los medios informáticos como valor fundamental, para la informática y la justicia.

Por lo tanto se puede decir que la informática forense es es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional colección y análisis de datos provenientes de un sistema de cómputo, una red, un sistema de comunicaciones y un medio de almacenamiento masivo.

Por otra parte es importante dar una definición de evidencia digital, porque este término está relacionado con la informática forense, es así que Casey define a la evidencia digital como "cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar un enlace (link) entre un crimen y su víctima o un crimen y su autor". [12]

Siendo que la evidencia digital es un dato que puede ser utilizado como un medio probatorio de un delito, el tratamiento del mismo debe seguir un procedimiento que le dé la validez necesaria; por lo tanto se debe recurrir a un

modelo que pueda validar la evidencia digital; uno de los modelos planteados es el proceso PURI el cual se lo define en el siguiente párrafo.

El proceso PURI se define entonces como una secuencia de fases compuestas por etapas que involucran tareas a llevar a cabo para recuperar información almacenada digitalmente, aplicando técnicas implementadas en herramientas concretas que permiten ejecutar dichas tareas.[13]

Hasta este punto se puede observar que la informática forense tiende a recuperar la evidencia digital, pero para que esta sea valedera debe enmarcarse en un modelo que permita validar la evidencia recolectada, todo esto para probar la existencia o la no existencia de un delito informático.

Pero que es un delito informático, Nidia Callegari [1] define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas". Este concepto tiene la desventaja de solamente considerar como medio de comisión de esta clase de delitos a la informática, olvidándose la autora que también que lo informático puede ser el objeto de la infracción.

Julio Téllez Valdés [2] conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Por lo tanto el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los computadores.

Parker define a los delitos informáticos como "todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio" [3], Parker además entrega una tabla en que la que se definen los delitos informáticos de acuerdo a los propósitos que se persiguen:

A. Propósito de investigación de la seguridad

Abuso informático es cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia (Parker, Nycum and Oura, 1973).

B. Propósito de investigación y acusación

Delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática (Departamento de Justicia de Estados Unidos).

C. Propósito legal

Delito informático es cualquier acto tal como está especificado en una ley sobre delito informático en la jurisdicción en que la norma se aplica.

D. Otros propósitos

Abuso informático (sea cual sea su objetivo), es cualquier delito que no puede ser cometido sin computador.

Por lo tanto el delito informático es asociado con toda conducta ilícita que hace uso indebido de cualquier medio informático, susceptible de ser sancionada por el derecho penal, como también es una conducta típica, antijurídica y culpable en que se tiene a las computadoras como instrumento o fin. Este tipo de delito está íntimamente ligado a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información, etc.

Este es el marco teórico sobre el cual trabajaremos en el presente documento.

IV. SOLUCIÓN PROPUESTA

Para estructurar la solución propuesta, elaboraremos un análisis de las etapas en un proceso unificado para identificar cuál o cuáles son las etapas más críticas en la recolección de la evidencia digital; de acuerdo a este análisis gestionaremos el riesgo utilizando el enfoque del software libre, con ayuda de un modelo matemático, el cual nos permita estructurar de forma adecuada el modelo propuesto en el presente artículo.

i) Etapas en un proceso unificado.

A. Fase de adquisición.

Esta fase comprende toda actividad vinculada con la generación de una réplica exacta de todo el contenido digital alojado en el dispositivo original.

La fase de adquisición comprende etapas que de acuerdo al entorno en el que se deba llevar a cabo la recuperación de la información. Es así que se procede a dividir la adquisición de dispositivos por sus características altamente diferenciadoras a todo nivel, tanto físico (hardware), cómo lógico (software).

B. Fase de Preparación.

Esta fase involucra todos los procedimientos necesarios para generar el entorno de pruebas, es preciso para llevar a cabo en primer lugar la inspección, y eventualmente la recuperación de la información.

Como primera etapa, la fase de preparación contempla la restauración de la imagen. Esto significa que si la misma se encontrara dividida, encriptada o comprimida deberá realizarse el proceso contrario, a fin de lograr el original.

A continuación se deberá validar que la restauración si ha sido exitosa mediante un algoritmo de hash.

Si la imagen que se obtuvo es de un sistema de archivos de un determinado sistema operativo, entonces será útil generar una máquina virtual que tome dicha imagen como su disco principal.

Al hacerlo se debería realizar una copia a fin de no alterar la imagen original.

Finalmente esta etapa contempla la identificación de tipos de sistemas de archivos y sistemas operativos contenidos en los medios de almacenamiento originales.

C. Fase de Análisis.

Esta fase comprende el fuerte del trabajo en donde se analiza el contenido adquirido en busca de vestigios de lo que se quiere hallar. El objetivo final de la fase de análisis en el caso de un proceso judicial o pre-judicial es encontrar la denominada evidencia digital, es decir, aquello que relaciona el hecho ocurrido con el "imputado" y la "víctima". Entonces, se piensa en la evidencia digital como en un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales.

La fase de análisis comprende las siguientes etapas:

i) Extracción lógica
ii) Extracción física
iii) Análisis de relaciones

La extracción lógica representa la recuperación de información eliminada a partir del sistema de archivos. Por esa razón se denomina "lógica", ya que no se accede en forma directa a los bloques, sino a través del sistema de archivos, y del sistema operativo como intermediario.

La extracción física, en cambio, va directo al dispositivo, eludiendo el sistema operativo. La mayoría de los sistemas operativos no eliminan la información en el momento en el que un usuario solicita el borrado de un archivo determinado, sino que, de alguna manera, dejan registrado que el espacio que ocupaba dicho archivo ahora se encuentra disponible. De esta manera, por ejemplo, si fuese posible hallar tal espacio entonces sería posible reconstruir la información original.

La etapa de análisis de relaciones trata justamente de identificar relaciones entre conjuntos de archivos, con el fin de obtener una conclusión. Esto involucra puntualmente la Identificación de relaciones entre conjunto de archivos vinculados a una actividad en particular (ej: archivos relacionados a la navegación por internet) y la verificación de aplicaciones instaladas, entre otros.

Un punto interesante es comparar el proceso PURI con las guías de procedimiento mencionadas, sin embargo, este objetivo excede la finalidad de este artículo.

Estas fases son también aplicadas en un entorno del software libre, ya sea que las herramientas utilizadas sean aplicadas en el entorno del software libre o nos encontremos en el caso de analizar un dispositivo que utilice software libre.

Luego de analizar de las etapas de un proceso unificado, se realizará un análisis de los aspectos más críticos de la fase de extracción de datos, en el tratamiento de la evidencia digital.

ii) Aspectos carentes detectados en las etapas de un proceso unificado.

Uno de los procesos de mayor criticidad es la fase de análisis, en donde se tiene la extracción física, la extracción lógica y el análisis de relaciones.

De acuerdo a este análisis se plantea como solución extraer la evidencia digital utilizando el algoritmo planteado por File Carving.

Se observa que el proceso de la extracción de la evidencia digital es un proceso es muy delicado y que debe ser tratado con mucha diligencia, para ello proponemos la utilización del File Carving en el proceso de extracción de archivos u objetos del disco en ausencia de metadatos del sistema de archivo, es decir, accediendo directamente al contenido de los bloques [14]. El proceso de file carving se basa en recuperar información que ha sido eliminada o es inaccesible debido a daños del dispositivo o del sistema de archivos. Su uso es vital en la Informática Forense, ya sea para recuperar archivos eliminados que puedan ser utilizados como prueba, como para recuperar información comercial o personal valiosa. [15]

Existen varias técnicas de File Carving, algunas implementadas en herramientas, y otras ún no.

Estas técnicas varían desde las más básicas, basadas en la lectura del header y footer de un archivo, hasta otras mucho más complejas como Bifragment Gap (Garfinkel), Smart Carving (Pal, Memon etal) o Semantic Carving (Garfinkel). Incluso algunas tienen varios enfoques, como por ejemplo Header/Footer carving que puede aplicarse en una sola o en múltiples pasadas.

El proceso de File Carving ha ido evolucionando en los últimos años, sin embargo no cuenta aún con una definición flexible, adaptable e integradora, que permita describir y utilizar las técnicas que mejor se adapten a cada estructura de archivos.

Como parte del desarrollo se implementaron dos soluciones de preprocesamiento, cuatro algoritmos de file carving, dos soluciones de postprocesamiento y un logger de extracción, junto con otros objetos asociados que fueron necesarios para mantener un equilibro entre el nivel de abstracción deseado en cada parte y el rendimiento del producto. Es destacable que, si bien se mantuvo un alto grado de abstracción que permite la fácil implementación de

algoritmos de carving y componentes de pre y postprocesamiento, el rendimiento no tuvo un impacto significativo, y en condiciones similares es posible acercarse al rendimiento de "Scalpel", reconocido por su foco en la alta performance y bajo consumo de recursos. [16]

Con respecto a los algoritmos de carving, se implementaran tres variantes de header/footer carving y se analizará una implementación de carving basado en la estructura interna de archivos, algunas herramientas desarrolladas en software libre utilizan File Carving en el análisis de la extracción de datos de un determinado dispositivo de almacenamiento de datos.

V. Sujetos Del Delito Informático

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo

i. Sujeto activo

Se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal.

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos (Nros. 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada (Insiders). Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones informáticas cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa (Outsiders). [5]

ii. Sujeto pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.

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

iii. Bien jurídico protegido

El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir –ya que constituye la razón de ser del delito– y no suele estar expresamente señalado en los tipos penales.

El bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

- *El patrimonio*, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.
- *La reserva, la intimidad y confidencialidad de los datos*, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.
- *La seguridad o fiabilidad del tráfico jurídico y probatorio*, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.
- *El derecho de propiedad*, este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático.

Para los autores chilenos Claudio Magliona y Macarena López, sin embargo los delitos informáticos tienen el carácter de complejos, es decir "que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo".[6] En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos.

Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

VI. Situación Internacional

Durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

VII. SITUACIÓN NACIONAL

En Bolivia, para hacer frente a la delincuencia relacionada con la informática, se adoptó la estipulación del delito informático en la *ley 1768 conocida como el Código Penal Boliviano* en donde se consideran las siguientes figuras penales, encontrándose cada una de ellas en sus respectivos artículos, ellos son:

- *Artículo 363 bis.- (Manipulación informática)*

El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Realicemos un análisis del Artículo 363 bis (Manipulación informática).

En la reforma del código penal se ha introducido esta figura por el desarrollo de la informática que ha ido evolucionando de forma progresiva. La tecnología con el empleo de procedimientos precisos y rápidos que usados legalmente alivian el trabajo y dan mayor seguridad en la obtención de datos, también la misma usada ilícitamente da lugar a la comisión de delitos a veces de gran volumen.

Este delito es de resultado por su naturaleza y por decisión de la ley porque si no hay resultado no hay una transferencia patrimonial ilícita, no hay consumación pero puede darse la tentativa, es decir realizar la manipulación pero no alcanzar el fin propuesto. En cierto modo se parece el enriquecimiento ilícito o sin causa justa.

Es delito que excluye toda posibilidad de culpa. La antijuricidad radica en que intencionalmente se manipula datos informáticos para lograr resultados incorrectos o evitar un procesamiento correcto a fin de lograr de modo ilícito una transferencia patrimonial en perjuicio de tercero que sufre un detrimento patrimonial, es por esta razón que se ha incluido entre los delitos contra la propiedad.

La manipulación de datos en manejarlos alternado el procesamiento o haciéndolos errar desviando el resultado verdadero, lo que evidentemente en muchos casos como en cuentas bancarias determinan transferencias incorrectas mermando el patrimonio de terceros o de los mismos bancos.

Por lo que:

Sujeto activo: Cualquier persona (presidentes de bancos, ingenieros en sistemas, ingenieros electrónicos, programadores, operadores de terminales y otros).
Sujeto pasivo: Persona afectada o sector afectado (mundo de los negocios).
Delito: Impropio
Elemento Subjetivo: Dolo

C.S.Q.: - Manipule datos informáticos para lograr resultados incorrectos o evitar un proceso correcto a fin de lograr ilícitamente una transferencia patrimonial.

- En perjuicio de un tercero.

Verbo nuclear: Obtener, manipular.
Bien jurídico protegido: La propiedad.
Sanción: Reclusión de 1 a 5 años y multa de 60 a 200 días.

- *Artículo 363 ter.- (alteración, acceso y uso indebido de los datos informáticos)*

El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

Así mismo, la *Constitución Política del Estado plurinacional de Bolivia*.

- Sección III: Acción de protección de privacidad

Artículo 133

I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal y familiar, a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

Artículo 134

I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

III. La decisión se elevará en revisión de oficio ante el Tribunal Constitucional Plurinacional, en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.

IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo a lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme a lo dispuesto por este artículo, quedará sujeta a las sanciones previstas por la ley.

Se puede observar que los delitos informáticos son abordados desde un punto de vista secundario y casi no son nominados de esta forma directa, en la *ley de telecomunicaciones* que en el Título IV capítulo II, hace referencia al gobierno electrónico y software libre, Artículo 77 (software libre), en donde todavía no se hace el tratamiento de los delitos informáticos. En el capítulo tercero el de los documentos y firmas digitales, tampoco se toma en cuenta los delitos informáticos; es más en el capítulo cuarto se hace referencia al comercio electrónico en donde en el Artículo 88 (Controversias) se dice que si existiesen se debería acudir a la jurisdicción ordinaria; esto quiere decir a la ley 14379 que es el código de comercio boliviano y si se daña algún bien jurídico protegido se recurrirá al código penal boliviano y se lo tipificará de acuerdo al delito que se haya cometido.

Por lo tanto una ley dedicada a lo que son los delitos informáticos no se tiene en Bolivia, solo se tienen leyes diferidas de acuerdo a cada uno de los casos en los que se vayan a tipificar.

Realizando todo este análisis se puede observar que no existe en nuestra legislación la figura legal de la evidencia digital y menos existe una sanción a este tipo de acciones antijurídicas.

VIII. CASOS NACIONALES

De acuerdo a la investigación que se hizo se encontró un caso que llego a obtener una sentencia constitucional; el caso se pasa a detallar en las siguientes líneas:

- *Delitos informáticos en Bolivia*

En el Tribunal Constitucional podemos encontrar Recursos interpuestos ante esta instancia relacionada a "delitos informáticos" (Código Penal Art. 363bis Manipulación Informática y 363ter Alteración, acceso y uso indebido de datos informáticos), los más interesantes son los siguientes de los cuales realizo una extracción de los aspectos que considero más relevantes:

SENTENCIA CONSTITUCIONAL Nº 1177/01-R
Distrito: Santa Cruz

Supuestos Delitos: Estafa, falsedad ideológica, abuso de confianza, apropiación indebida, asociación delictuosa, manipulación informática, y alteración y uso indebido de datos informáticos.

Institución financiera: Fondo Financiero Privado “AAA” S.A.
Recurso presentado: Hábeas Corpus por detención ilegal y procesamiento indebido, pide inmediata libertad a su representado.

Argumentos Acusado: • No existe firma del Fiscal como tampoco del Policía que recibió "la supuesta declaración" • No se ha notificado al imputado con las supuestas querellas que existen en su contra, habiéndole privado de su derecho a la defensa.

SENTENCIA CONSTITUCIONAL 1075/2003-R
Distrito: Cochabamba

Supuestos Delitos: Manipulación informática Juicio oral penal ante el Tribunal de Sentencia Tercero de Cochabamba Institución financiera: Banco “BBB” S.A.

Recurso presentado: Hábeas corpus alegando la vulneración del derecho a la doble instancia, solicita se disponga la nulidad del Auto de Vista que declara inadmisible su apelación.

Resultados: • El 18 de noviembre de 2002, se dictó sentencia que la condena a tres años y cinco meses de reclusión: Interpuso recurso de apelación restringida • El recurso de apelación restringida se declaró inadmisible su apelación con el argumento de no haber cumplido con los requisitos formales: Quedó la acusada en plena indefensión y tutela efectiva con su recurso. • Declarar PROCEDENTE el recurso de Hábeas Corpus planteado.

SENTENCIA CONSTITUCIONAL 0296/2005-R
Distrito: Santa Cruz

Supuestos Delitos: Estafa agravada y manipulación informática Penas: 3 a 10 años Institución financiera: Cooperativa de Ahorro y Crédito “CCC Ltda.”

Recurso presentado: Habeas Corpus contra el fiscal de Materia para la suspensión de la orden de aprehensión de la acusada.

Denuncia: La nombrada a través de artificiosas manipulaciones e información de documentos, y

aprovechando su condición de responsable del procesamiento de información crediticio y en su condición de Jefa de Crédito de la Cooperativa de Ahorro y Crédito "CCC" Ltda., logró desviar dineros en beneficio personal en la suma de $us169.600.- en coordinación con otras dos personas con quienes tenía cuenta de ahorros mancomunada.

Argumentos Acusada: • El delito de estafa agravado implica multiplicidad de víctimas • No podían acusar a su representada de estafa agravada, por cuanto no se reunió con el Directorio ni hizo incurrir en error a los socios de la Cooperativa, no existió relacionamiento directo entre estafador y víctima.

Resultados: • Declarar IMPROCEDENTE el recurso.

CONCLUSIONES: Del análisis de estos y otros casos, podemos concluir:

* Si bien en el presente artículo sólo se mencionan 3 instituciones, esto no quiere decir que en las demás instituciones financieras no existió por lo menos un "delito informático", el que esté libre de este mal que tire la primera piedra. Muchos de los casos no llegan ni a la etapa de denuncia por cuidar la Imagen de la Institución y no afectar la confianza del público.

* Cuando se imputa a una persona por un delito informático, generalmente el 363 bis Manipulación Informática (sólo este tiene pena de cárcel), la imputación incluye además otros delitos con más o menos años de cárcel, por ejemplo abuso de confianza, hurto, uso de instrumento falsificado, estafa agravada, etc. Esto se da porque si bien se pueden manipular los datos de entrada, el proceso o la salida de datos, estos datos en algún momento se reflejan en un papel firmado/rubricado o para causar el daño patrimonial establecido en el 363 bis, alguien deberá recibir el dinero físicamente.

* Los delitos informáticos en muchos casos no se castigan por defectos procesales, al igual que otro tipo de delitos, en este punto debemos resaltar la falta de capacitación del Personal de la fuerza de la Ley (policía y fiscales) en el secuestro de evidencia digital y la preservación de la cadena de custodia de la misma.

* En los últimos tiempos existe un auge de peritajes informáticos (será efecto de la serie de televisión CSI?), quizá no tanto porque se cometen más delitos informáticos, sino más bien por la tecnificación de los delincuentes, cometen los mismos delitos con ayuda de la tecnología.

* Como consecuencia del desconocimiento de las Nuevas Tecnologías por parte de la mayoría de los Jueces y Fiscales, existe una excesiva dependencia que recae en los "Peritos Informáticos" y esto no solamente se da en Bolivia, por ejemplo en Argentina varios de los expositores en el VII Seminario sobre Delitos en Tecnología, también se manifestaron al respecto.[9]

IX. ESTADÍSTICA CASOS NACIONALES

De acuerdo a una de las publicaciones de un diario nacional, se obtuvieron las siguientes estadísticas:

Entre 2003 y 2007, la fuerza anticrimen recibió 185 denuncias de manipulación informática y de alteración, acceso y uso indebido de datos en toda Bolivia, pero se desconoce si alguna de ellas fue resuelta.

Los datos de la Fuerza Especial de Lucha Contra el Crimen (FELCC) revelan que en Santa Cruz, La Paz y Cochabamba se producen más delitos informáticos desde 2003.

Desde ese año hasta 2007, la Policía registró un total de 185 fraudes electrónicos en todo el país, de éstos, 177 corresponden a manipulación informática y ocho a alteración, acceso y uso indebido de información. De la primera figura legal, 91 casos hubo en Santa Cruz, 46 en Cochabamba, 30 en La Paz, cuatro en Potosí, tres en Oruro, dos en Beni y uno en Tarija.

Sobre alteración informática, tres ocurrieron en La Paz, dos en Cochabamba, dos en Beni y uno en Santa Cruz. Entre enero y septiembre de este año hubo 50 denuncias de manipulación electrónica (27 en Santa Cruz, 12 en La Paz, nueve en Cochabamba y dos en Chuquisaca) y ninguna acerca de alteración. [10]

De 2002 a 2011, los juicios por delitos informáticos crecieron en 890%, de ocho a 79, de los cuales 62 están referidos a manipulación informática y 17, a la alteración, acceso y uso indebido de datos informáticos. Aparte, en esa década, los juzgados paceños recibieron 228 causas referidas al primer delito y 15 del segundo. Asimismo, en los cuatro meses que van de este año, ya se ventilan 29 causas: 27 que incumben al artículo 363 bis y dos al artículo 363 ter del Código Penal. [11]

- *Análisis del porque crecieron tanto los delitos informáticos*

Para entender cómo combate la Policía los delitos informáticos o cibernéticos, y cuáles son sus limitaciones, nada mejor que la opinión de quien comanda a nivel nacional la Fuerza Especial de Lucha Contra el Crimen (FELCC), el coronel Jorge Toro, quien señala que su repartición incluso tiene que lidiar con la falta del servicio de internet para investigar estos casos.

Las denuncias más comunes que la FELCC recibe sobre delitos informáticos son las amenazas por celular se dan a diario y lo único que se hace es la extracción de los mensajes, no la investigación de dónde provienen, por falta de tecnología.

Para efectivizar el trabajo que realiza la FELCC falta que se comuniquen entre las 62 oficinas de la FELCC que operan en el país. Los delincuentes trabajan en red o se mueven de un

lugar a otro y la FELCC no tiene ni la instalación de internet, pero inclusive así trata de hacer cualquier cosa para poder investigar. “Los delincuentes están volando y nosotros vamos a pie”, estas declaraciones le corresponden al coronel Jorge Toro, funcionario de la FELCC.

La solución sería implementar un laboratorio de informática actualizado, que costaría alrededor de 20 mil dólares.

Por lo tanto si la policía no está con las condiciones adecuadas de combatir este tipo de delincuencia, será muy difícil el combatirla.

Parte de la solución integral depende de las políticas de estado, el gobierno debería observar este tipo de datos alarmantes para tomar las medidas necesarias.

IX. CONCLUSIONES

En los últimos años, las sociedades en todo el mundo han experimentado un cambio progresivo en el que cada vez más se depende de sistemas informáticos para manipular información. Este cambio se debe, entre otras cosas, al aumento en la cantidad de información con la que se cuenta, a la transferencia de procesos tradicionales a sistemas informáticos, servicios y productos que buscan, simplificar tareas de la vida moderna.

Los cambios en las tecnologías, plataformas, medios de almacenamiento, legislaciones y aplicaciones de software, hace cada vez más necesario el uso de procesos, métodos, estándares y buenas prácticas que permitan garantizar la recuperación de información contenida, y sobre todo, que permitan asegurar que se realizaron todas las tareas posibles con los mecanismos adecuados.

Se plantea realizar una delicada tarea diligente en la fase de análisis, en las etapas de extracción lógica y física de los datos en los dispositivos de almacenamiento de datos.

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro.

Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

En conclusión podemos decir que el bien jurídico protegido en general es la información, pero esta considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan.

Por tanto el bien jurídico protegido se acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

Los delitos informáticos constituyen una nueva forma de delinquir que debe ser regulada.

Los sujetos, tanto activo como pasivo, tienen características propias.

Si el mundo digital ha sido un caldo de cultivo para este tipo de delincuencia, el ciberespacio lo es más, y la importancia del tema crece vertiginosamente, estar detenidos no es equivalente a no avanzar, es equivalente a retroceder, por lo tanto debemos recurrir a un modelo que permita validar la evidencia digital y esta sea utilizada como un medio probatorio ante un hecho delincuencial.

Para ello debemos recurrir a algoritmos matemáticos que permitan validar la recuperación de la información en un medio de almacenamiento, por lo tanto recurriremos a herramientas desarrolladas en software libre que utilizan File Carving en el análisis de datos.

Finalmente no existe una figura jurídica que haga referencia a la evidencia digital en la legislación boliviana, se debe trabajar en el ordenamiento jurídico para que la misma sea considerada en nuestra legislación.

REFERENCIAS

[1] CALLEGARI, Nidia, Citada por Julio Telles Valdés. “Poder informático y delito ”,Ob. Cita.

[2] TELLEZ VALDÉS, Julio. “Los Delitos informáticos. Situación en México”, Informática y Derecho No 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.

[3] PARKER, D.B, Citado por Romeo Casabona Carlos M. Poder Informático y Seguridad Jurídica.

[4] HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio, Los Delitos Informáticos, Editorial Jurídica Cono Sur.

[5] SUTHERLAND Edwin, Citado por Tiedemann Klaus, Poder Económico y delito.

[6] REYES ECHANDÍA, Alfonso, La Tipicidad, Universidad de Externado de Colombia, 1981.

[7] GUIBOURG Ricardo A., ALENDE Jorge O., CAMPANELLA Elena M., Manual de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires, Argentina.

[8] CAMACHO LOSA, Luis, El Delito Informático, Madrid, España, 1987.

[9] http://www.buenastareas.com/ensayos/Delitos-Informaticos-En Bolivia/3735918.html, Miércoles 8 de octubre de 2008

[10] http://www.telecombol.com/2008/12/cincuenta-delitos-informticos-estn-sin.html

[11]http://www.la-razon.com/suplementos/informe/Paz-juicios-delitos-informaticos-crecieron_0_1609639058.html,

[12] Casey, E. (2001) Handbook of Computer Crime Investigation. Academic Press.

[13] Cano, Jeimy J. (2003). Introducción a la Informática Forense. Revista de Derecho Informático Alfa-Redi. Consultado el 28 de octubre de 2011 en la www:http://www.alfa-redi.org.

[14] MEROLA A.: Data Carving Concepts, SANS Institute (2008)

[15] CONSTANZO, Bruno; WAIMANN, Julián El estado actual de las Técnicas de File Carving y la necesidad de Nuevas Tecnologías que implementen Carving Inteligente. Journal CADI (2012).

[16] GOLDEN G. RICHARD III, VASSIL ROUSSEV, "Scalpel: A Frugal, High Performance File