La suplantación de identidad

de tipo físico, informático y de telecomunicaciones como nueva manifestación de las conductas antisociales

COLECTIVO ARCION

Surge en el año 2008, equipo interdisciplinario de investigadores en el campo de lo Criminológico-criminalístico, su actividad científica coadyuva al desarrollo y consolidación del modelo educativo CLEU. "Investigar para la libertad". Representa su filosofía de batalla.

> "La mayoría de los países no cuentan con una clara definición respecto del delito de robo de identidad, ilícito del que se valen algunos grupos de la delincuencia organizada y de terroristas para facilitar y financiar sus actividades"
>
> *Donald Piragoff*

RESUMEN

La inevitable revolución tecnológica modifica el *modus vivendi* de millones de personas, que manifiestan una manía al uso de telefonía móvil, ordenadores, tabletas electrónicas, *Ipods*, entre otros, donde el uso del internet es casi indispensable, pero muy cerca de ellos y a la par de la tecnología se encuentra el sujeto que se aprovecha de la vulnerabilidad de la víctima, y es entonces el momento justo donde se desarrolla la suplantación de identidad.

INTRODUCCIÓN

El ser humano está dotado de derechos y obligaciones, todo ello por el simple hecho de nacer dentro de un territorio nacional, dichos beneficios son otorgados por el Estado y es responsabilidad del ciudadano corresponder al beneficio.

La identidad es un beneficio otorgado por el Estado para la ciudadanía, ya que corresponde a éste otorgar los recursos necesarios para generar documentos oficiales que acrediten los datos personales de los solicitantes, por ello es que cada integrante de las poblaciones cuentan con documentaciones que demuestren su nacionalidad, lugar de nacimiento, fecha de nacimiento, y número de control dentro de los registros de cada entida.

Hoy en día, la delincuencia busca diversas situaciones que pueden ser bien aprovechadas para cometer delitos o simplemente para perjudicar a sus semejantes, como muestra de este acontecimiento, la suplantación de identidad, fenómeno que retoma fuerza por la vulnerabilidad y confianza de la población, este procedimiento sucede cuando simplemente a través de la telefonía la víctima acepta brindar cualquier información que le solicita el moderador, sin razonar plenamente que se puede tratar de un sujeto que utilice dicha confidencialidad para obtener beneficios económicos o patrimoniales que son fruto del esfuerzo del trabajo de la ciudadanía.

Los malhechores tienen gran ingenio para cometer sus fechorías y recibir enormes cantidades de dinero sin la necesidad de enfrentar a sus víctimas o utilizar la violencia para obtener lo que desean, tan solo basta con robar

los bolsillos o carteras para conseguir tarjetas de crédito, débito, identificaciones personales, claves bancarias entre otras más, o simplemente sentarse detrás un ordenador para conseguir claves o interferir en la intimidad de millones de personas que descuidan su información confidencial.

Con base a las denuncias y quejas realizadas por la ciudadanía, es como se llegó a obtener las diversas modalidades de la suplantación de identidad, y éstas son:

- Físico.
- Informático.
- De telecomunicación.

Actividades como la clonación de tarjeta, alteración y falsificación de documentos oficiales de identidad, envío de mensajes vía internet o celular anunciando supuestos sorteos o concursos, o *hackeo* de cuentas, son tan solo algunas de las actividades derivadas de la suplantación de identidad.

Esta conducta antisocial permite favorecer ciertos delitos como el caso del tráfico de personas, terrorismo, usurpación de funciones, falsificación y alteración de documentos en general, lavado de dinero, entre otros, por ello debe atenderse con prontitud la problemática que afectó de manera indirecta gracias a la tecnología o de algunas artimañas de la delincuencia.

ROBO DE IDENTIDAD

Una de las actividades ilícitas que ha trascendido de manera considerable en algunos países, es el llamado robo de identidad o mejor conocido como *identity theft* (voz inglesa). Apropiación ilegal de identidad. Este fenómeno delictivo afecta en algunos casos de manera inmediata a las víctimas que lo padecen, y en otros casos las repercusiones se manifiestan a largo plazo, ejemplo de ello, cuando una persona utiliza la identidad de otra para realizar una solicitud de crédito, procedimiento que es desconocido por la víctima, pero a mediano plazo ésta empieza a recibir notificaciones de la deuda existente por un crédito que jamás solicitó, o en casos extremos le es comunicada que es perseguida por la justicia.

La parte afectada en esta problemática sin lugar a duda es la víctima, quien pierde de manera específica, su identidad legal, su estabilidad económica, en casos extremos su libertad, y principalmente se encuentra ante un inevitable daño moral, donde su prestigio o su imagen se ven completamente dañadas ante los ojos de la sociedad o de la justicia.

Para dar prioridad a la demanda de la ciudadanía que ha sido víctima de robo de identidad y por la magnitud de éste, así como la amenaza que representa para la población, algunos países han puesto su atención y conciben de manera específica a esta conducta como "un crimen federal que ocurre cuando la identificación de la persona es utilizada o transferida por otra persona para actividades ilegales"[1].

Entre las actividades más destacadas por este delito se encuentra las siguientes:

- Quejas relacionadas con el robo de identidad.
- "Fraude con Tarjetas de Pago.
- Servicios no Autorizados de Servicios Públicos o Teléfono.
- Fraude Bancario.
- Préstamos Fraudulentos.
- Documentos o Beneficios Gubernamentales.

Estafas de robo de identidad más utilizadas:

- Sorteos falsos u obras de beneficencia falsificadas.
- Trabajos en el hogar que ofrecen ganar dinero fácil.
- Tarjeta de pago, protección de crédito u ofertas de reparación de créditos falsos.
- Ofertas de viajes a tarifa reducida u ofertas con descuento en revistas.
- Estafas de Becas"[2].

Otra forma de delinquir realizada a nivel mundial, derivada de la obtención de datos personales para actividades ilegales, es el delito informático, definido como "Cualquier comportamiento criminal en que la computadora u otros periféricos o dispositivos informáticos, estén involucrados como material, objeto o símbolo para perpetuar un fraude, engaño, o delito informático tipificado"[3].

Por su parte Estados Unidos, Canadá, y la mayoría de los países Europeos, han determinado que existen tres tipos de comportamiento ilícito relacionado con los delitos informáticos:

- Acceso no autorizado.
- Actos dañinos o circulación de material dañino.
- Intercepción no autorizada.

Estos tres tipos fueron tipificados y penalizados por los sistemas legales de aquellas naciones, pero desde el punto de vista criminológico algunos autores clasifican a los delitos informáticos desde dos variantes:

- Como instrumento o medio.
- Como fin u objetivo.

Estas dos apreciaciones se entienden de la siguiente manera:

Como instrumento o medio: se tiene como manifiesto aquellas conductas criminógenas que utilizan la tecnología para utilizarla como artificio para ejecutar actividades ilícitas.

Como fin u objetivo: En esta etapa las conductas criminógenas rechazan la presencia de la computadora o programa entendido como entidad física, mientras que por su parte otros conciben a esta como una clasificación *sui géneris*, como los llamados -delitos electrónicos-, mismos que se dividen en tres categorías:

1. Individuos que a beneficio utilizan la tecnología electrónica como un método, es decir, esta vía es un medio cuyo objetivo es llegar a consumar una actividad ilícita.

1 Slideshare present yourself 'Robo de identidad/ identity theft/ Apropiación ilegal de identidad Rivera Suárez, Waleska'. [En línea]. [Consultado: 12 de enero de 2012]. Disponible en la web: http://www.slideshare.net/waleska123/robo-de-identidad-5323179

2 Master card 'Robo de identidad'. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: http://www.mastercard.com/us/personal/es/basicosdeseguridad/robodeidentidad/

3 Scribd. 'Unidad lll. Seguridad informática. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: http://es.scribd.com/doc/20781206/Delitos-Informaticos

2. De aquellas personas que a través innovación de la tecnología electrónica usan la computadora como herramienta principal para cometer sus fechorías.
3. Los que se valen del avance tecnológico para cometer un solo fin: dañar el medio electrónico.

La seguridad internacional se ha visto amenazada por intrusos del internet, que se introducen en los sistemas para robar información confidencial y vulnerar al país, como el tan famoso gusano de internet proyectado en Estados Unidos de América en el año de 1988 por Robert Morris Jr., mismo que fue detenido y sancionado gracias a la existencia del acta fraude y abuso informático que circulaba durante esa época.

Los delitos informáticos han atormentado la economía de diferentes países, como el caso de Estados Unidos de América, que su pérdida económica alcanza los 10,000 millones de dólares, esta información es brindada por las compañías de seguros contratadas por estas potencias mundiales, mismas que registran que es tan grande el daño y perjuicio económico que se propone crear grupos exclusivos de investigadores especializados en delitos informáticos.

Tan solo el *Federal Bureau of Investigation* (FBI). Oficina Federal de Investigaciones, ha atendido tan solo el 90% de los delitos informáticos perpetrados en los Estados Unidos de América vía internet.

Las redes de comunicación hoy en día, se han vuelto una necesidad, y no un lujo, como se creía en épocas pasadas, ahora accesar a internet significa fuente de empleo, comunicación, transacciones, desarrollo, publicidad, imagen, entre otras cosas.

Una de las herramientas indispensables en ésta época es la llamada red de comunicación mejor conocida como internet, el cual no estaba diseñado para las inferencias criminales de los últimos años, los protocolos con los que se cuenta no se encuentran protegidos, por ello es que en la actualidad, se puede observar ataques contra la seguridad por parte de *hackers*.

Otro tema de seguridad es el uso inapropiado de la "criptología"[4] a favor de la delincuencia para ocultar mensajes que pueden ser ininteligibles para los demás así como para ocultar movimientos realizados en un sistema informático, e inclusive se puede ocultar exactamente lo que se estaba realizando ya que dicha información se encuentra encriptado. Otra forma de realizar un ataque informático es mediante los llamados "cripto-virus"[5].

Ante esta problemática las legislaciones internacionales han integrado dentro de sus ordenamientos incluir la suplantación de identidad de tipo electrónico mismo que a la letra dice:

Nuevo Código Penal Español (aprobado por Ley-Orgánica 10/1995, de 23 de noviembre / BOE número 281, de 24 de noviembre de 1995):

1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Con base a ello la Organización de las Naciones Unidas a través de un manual denominado la prevención y control de los delitos informáticos número 43 y 44 informa que el 90% de los casos detectados por delito informático fueron realizados por los propios empleados de las empresas denunciantes, mientras que dentro de América Latina y Europa el 73% de los delitos consumados por esta modalidad fueron realizados por fuentes internas a empresas y tan solo el 23% de los hechos fueron señalados por personas ajenas a las empresas.

Convenios internacionales para prevenir el robo de identidad por internet

El mal uso de los ordenadores han producido en el ámbito internacional realizar una correcta valoración político-jurídico donde se ha admitido modificar el derecho penal nacional.

Para ello se cuentan con ciertos convenios internacionales realizados para combatir la suplantación de identidad vía internet:

- El Convenio de Berna.
- La Convención sobre la Propiedad Intelectual de Estocolmo.
- La Convención para la Protección y Producción de Fonogramas de 1971.
- La Convención Relativa a la Distribución de Programas y Señales.

En el año de 1983 la Organización de Cooperación y Desarrollo Económico (OCDE), comenzó a realizar un estudio para reordenar las leyes penales a fin de tipificar aquellas actividades donde se realice un mal uso de programas de computación.

Esta problemática determina ampliamente una implicación económica que deja la delincuencia por el mal uso de un ordenador, su daño no queda únicamente dentro de las naciones, sino que es un problema de carácter internacional e incluso transnacional, motivo que incita a las autoridades a unificar las legislaciones para combatir este problema.

En el año de 1986 la OCDE realizó un informe que fue publicado bajo el nombre de –Delitos de informática: análisis de la norma jurídica-, mismo que indicaba las normas legislativas vigentes así como las nuevas propuestas a reformas que debe adoptar los Estados, así como algunas actividades. Durante el año de 1992 esta organización realizó un conjunto de normas dirigidas hacia la protección de la información con la finalidad de ofrecer las bases para que los Estados y empresas del sector privado tengan alguna opción para realizar un marco legal que permita proteger la base de datos confidenciales.

Para 1990 la Organización de las Naciones Unidas (ONU), dentro de su octavo congreso celebrado en la Habana, Cuba, titulado

4 Criptología (del griego krypto: 'oculto' y logos: 'discurso') es, tradicionalmente, la disciplina científica que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas, Wikipedia, la enciclopedia libre 'Criptología'. [En línea]. [Consultado: 29 de enero de 2012]. Disponible en la web: Criptología http://es.wikipedia.org/wiki/Criptolog%C3%ADa

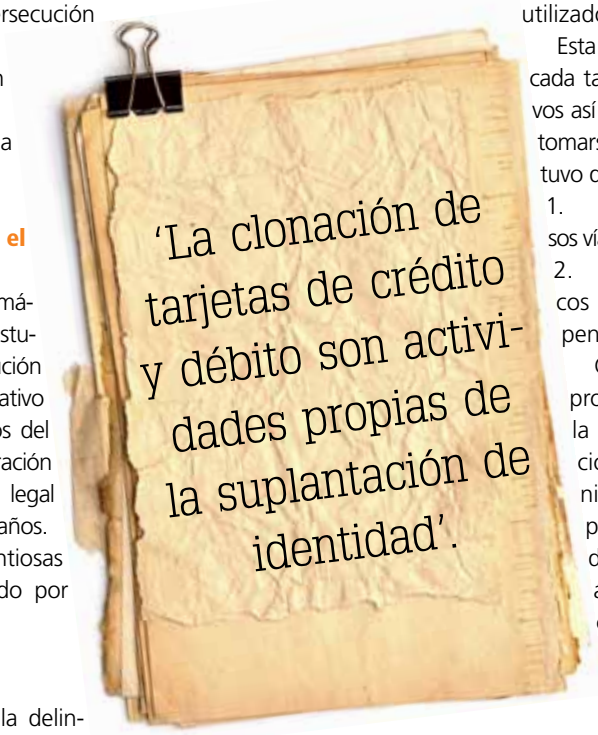
5 Cripto-virus. Programas con código vírico encriptados.

prevención del delito y justicia penal, se concluyó que la delincuencia relacionada con la informática simplemente es consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países, por ello se había difundido la comisión de actos delictivos.

En Wurzburgo durante 1992, la Asociación Internacional de Derecho Penal emitió recomendaciones con respecto a los delitos de tipo informático, entre ellas destaca la iniciativa de reformar el contenido penal y definir las nuevas conductas antisociales para ser tipificadas como delitos.

En Mérida España se celebró la II Jornada Internacional sobre –delitos cibernéticos- realizado en noviembre de 1997 donde se reveló lo siguiente.

- Aplicaciones en la Administración de las Tecnologías Informáticas/cibernéticas.
- Blanqueo de capitales, contrabando y narcotráfico.
- Hacia una policía Europea en la persecución del delito Cibernético.
- Internet: a la búsqueda de un entorno seguro.
- Marco legal y Deontológico de la Informática.



Las legislaciones mundiales contra el delito de robo de identidad

Las actividades ilícitas derivadas de la informática son un punto en concreto que debe estudiarse paso a paso y con su debida precaución implementando medidas de carácter legislativo y penal, por ello para países desarrollados del occidente se tuvo a bien realizar una valoración que incluye entre sus líneas una reforma legal que ha imperado durante los últimos diez años.

Este problema que ha generado cuantiosas pérdidas millonarias, sólo es vislumbrado por algunos países entre los más destacados:

Alemania

Alemania también fue perpetrada por la delincuencia informática, por ello contempló implementar una segunda ley dedicada a tipificar la criminalidad económica, todo ello ocurrido dentro del año de 1986 donde expresa lo siguiente:

- Espionaje de datos (202 a).
- Estafa informática (263 a).
- Falsificación de datos probatorios junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos. (269, 270, 271 y 273).
- Alteración de datos es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible. (303 a).
- Sabotaje informático. Destrucción de elaboración de datos de especial significado por medio de hecatombe, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa (303 b).
- Utilización abusiva de cheques o tarjetas de crédito (266 b).

Las autoridades alemanas detectaron una modalidad que se determinó como estafa informática y que fue incluido como un nuevo tipo penal, que en sus inicios tuvo algunas incongruencias, pero para demostrar su existencia debía cumplir con lo siguiente:

- Acción engañosa.
- Causa del error.
- Disposición patrimonial en el engaño del computador.

El resultado de este fenómeno es el daño directo que sufre la víctima en su patrimonio, por ello las autoridades elaboraron un programa contemplado la administración de datos por medio de un acto incorrecto del programa, esto con ayuda del uso de datos incorrectos e incompletos que han sido utilizados de manera ilegal

Esta expresión penal fue adjudicada también por países Escandinavos así como en Austria. Para poder tomarse en cuenta este delito se tuvo que estudiar:

1. Los comportamientos dañosos vía electrónica.
2. Analizar los bienes jurídicos merecedores de protección penal que eran dañados.

Con base a ello, se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero en realidad tan sólo constituyen un nuevo *modus operandi*, que no ofrece problemas para la aplicación de determinados tipos. Por otra parte, en cambio, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas. En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de sus sustancias o función de alteraciones de su forma de aparición.

Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987.
Esta ley contempla los siguientes delitos:

- Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
- Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Francia

Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

- Acceso fraudulento a un sistema de elaboración de datos (462-2). En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje informático (462-3). En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos (462-4). En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados (462-5). En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- Uso de documentos informatizados falsos (462-6). En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Estados Unidos de América

Es impotante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Toya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus. El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten sólo de manera imprudente la sanción fluctúa entre una multa y un año en prisión.

El Acta de 1994 aclara que el creador de un virus no escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje. En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley. Se considera importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10, 000 por cada persona afectada y hasta $50,000 el acceso imprudente a una base de datos, etcétera.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos. Es importante mencionar que en uno de los apartados de esta ley, se contempla la regulación de los virus (*computer contaminant*) conceptualizándolos aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

Holanda

El primero de marzo de 1993 entró en vigor la Ley de los Delitos Informáticos, en la cual se penaliza el hancking, el *preancking* (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

Reino Unido de la Gran Bretaña e Irlanda del Norte

Debido al caso de *hancking* en 1991, comenzó a regir la *Computer Misuse Act,* Ley de los abusos informáticos. Mediante esta ley el intento, exitoso o no de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Pena además la modificación de datos sin autorización donde se incluyen los virus.

Venezuela

En el año 2001 se promulgó la Ley Especial contra los delitos Informáticos por Asamblea Nacional de la República Bolivariana de Venezuela.

De los delitos Ccontra los sistemas que utilizan tecnologías de información, de los delitos contra la propiedad, de los delitos contra la privacidad de las personas y de las comunicaciones, de los delitos contra niños, niñas o adolescentes, de los delitos contra el orden económico, argumentados en cinco capítulos respectivamente. En las disposiciones comunes se abordan elementos importantes como las agravantes, las penas accesorias, la divulgación de la sentencia condenatoria etcétera.

Los Estados miembros de la Unión Europea acordaron castigar con penas de uno a tres años de prisión a los responsables de delitos informáticos. Cuando quede comprobado que los ataques cibernéticos están relacionados con el crimen organizado, la pena ascenderá hasta los cinco años. Esta decisión marco se convierte en un gran avance dentro de la armonización de las legislaciones europeas para luchar contra los delitos informáticos. Estos delitos se han convertido en un quebradero de cabeza para los cuerpos de policía de los Estados miembros y, sobre todo, para los perjudicados por estos crímenes. El principio de territorialidad del derecho provoca que sea muy complicado perseguir a delincuentes informáticos que actúan desde otros países.

Con este intento de unificar la legislación, las autoridades europeas podrán perseguir con una mayor efectividad a delincuentes que, hasta ahora, podían cometer sus delitos con casi total impunidad. Además, el acuerdo del Consejo de Ministros de Justicia de los quince, establece otro aspecto importante, como es la definición de los delitos que se consideran –informáticos-.

Los Estados miembros distinguen tres tipos de ataques cibernéticos: el acceso ilegal a sistemas informáticos, la ocupación de sistemas a través de ejemplos como el envío de mensajes que ocupan un espacio considerable, y la difusión de virus informáticos. La intención de la Unión Europea es doble: por un lado se trata de definir el delito; por otro pretende unificar las penas, ya que el lugar de la comisión del delito es fundamental para saber el derecho aplicable, se trata además de una medida muy sensata que evita la desprotección absoluta que presentan hoy en día las empresas del Viejo Continente. Los Quince Estados Europeos disponen ahora de un plazo de más de dos años para la adaptación de esta medida a sus textos legislativos.

El daño colateral para México

Los efectos que se desarrollaron en países como Estados Unidos, Argentina, Reino Unido, Alemania, entre otros, repercutieron de manera indirecta para México y vulneró la seguridad tanto del país como de los ciudadanos que habitan dentro de ella.

La tecnología que llega a manos de países tercermundistas son la fortuna que va llegando a México de manera gradual, lo más importante de ello son las herramientas como las computadoras de nueva generación, las *iPad* o tabletas electrónicas, entre otros, donde fácilmente se tiene acceso a internet, punto que es accesible para cualquier individuo que tenga conocimiento de ello, y tan solo basta con algunos dominios para hacer que las víctimas se vean vulneradas en sus datos personales, o en su estabilidad económica.

La era de la informática llega a manos de la sociedad, donde cualquier persona tiene acceso a un ordenador y al internet, y de manera virtual explora mundos desconocidos. Esta innovación se encuentra versada dentro de dos vertientes:

1. De beneficio social.
2. De acciones ilegales.

La primera de ellas resulta placentera y necesaria, ya que gracias al uso de un ordenador y del acceso a internet se facilita la socialización y la actividad laboral, este beneficio hoy en día, no está considerado como un lujo, si no como una herramienta de primera necesidad.

La segunda se encuentra encaminada hacia el acercamiento de la tecnología y las comunicaciones, misma que permite descubrir el talento de miles de hombres o mujeres jóvenes con gran capacidad para crear más que una simple escritura, tan solo basta con que se pueda manipular un programa de comunicación, un navegador o un gestor de correo para poder vincularlo en ocasiones con malas intenciones.

Esta actividad se encuentra prevista por muchos pensadores como -fuga de cerebros-, donde jóvenes con gran talento e inteligencia son guiados por personas malintencionadas hacia la comisión de conductas delictivas, y existe otra parte de la población joven que se inspira en los vicios de la red de internet, donde a través de ello se forman los grandes "*hackers*"[6].

6 Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etcétera. Se suele llamar 'hackeo y hackear' a las obras propias de un hacker.
El término 'hackers' trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.
Mirrorlinux.net, 'hacker'. [En línea]. [Consultado: 9 de enero de 2012]. Disponible en la web: http://mirrorlinux.net/index.php?option=com_content&view=article&id=93:hacker&catid=37:hack&Itemid=80

Los efectos en materia de informática que afectan a México son realmente considerables, y se clasifican de la siguiente manera:

"De impacto

Esta primera clasificación afecta directamente a la base de datos del gobierno sea éste municipal, estatal o federal, donde toda aquella información confidencial se encuentra expuesta ante los ojos de los genios informáticos mejor conocidos como *hackers*.

De afectación social

Este procedimiento tiene como repercusión el daño moral y patrimonial de la víctima a la cual le es suplantada su identidad, en muchas ocasiones el perjuicio se puede manifestar a largo plazo, donde la víctima pasa años sin saber que ha sido afectada, y en otras ocasiones puede observarse el daño de manera inmediata"[7].

México se encuentra vulnerable ante esta conducta antisocial, a la cual se le ha denominado -suplantación de identidad de tipo informático- y únicamente los argumentos jurídico-penales toma como referencia el delito de -Acceso ilícito a sistemas y equipos de informática-, donde entre algunas líneas principales se expresa lo siguiente:

"Artículo 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa[8]".

Como se puede observar este delito bajo el nombre de -Acceso ilícito a sistemas y equipos de informática- solo resguardan la información confidencial del Estado y de las Instituciones financieras, pero deja desprotegido la información con la que cuentan empresas y las demás personas del país.

Queda claro que la protección de los datos y de la identidad de las personas en medios informáticos se encuentra vulnerable ante la presente situación que se encuentra viviendo México, por ello es fácil realizar esta actividad que se realiza sin temor alguno.

La naciente legislación penal para la suplantación de identidad en México

Para México, la actividad de suplantación de identidad surgió de manera gradual, empezando por falsificación y alteración de documentos, como una forma de ocupar el lugar de otra, para posteriormente generar una crisis informática. Los factores físicos como la modificación y reproducción ilícita de documentos generó al hombre la gran idea de tener otra personalidad y mantener la propia, la que le fue legal y socialmente proporcionada, éste era una modalidad que no había sido tomada en cuenta y que progresivamente tendría la tendencia en convertirse en un fenómeno delictivo, las leyes Mexicanas hasta hace poco solo contemplaban como único hecho punitivo el fraude pero condicionalmente en las siguientes circunstancias:

"Artículo 387 fracciones:

II.- Al que por título oneroso enajene alguna cosa con conocimiento de que no tiene derecho para disponer de ella, o la arriende, hipoteque, empeñe o grave de cualquier otro modo, si ha recibido el precio, el alquiler, la cantidad en que la gravó, parte de ellos o un lucro equivalente;

III.- Al que obtenga de otro una cantidad de dinero o cualquiera otro lucro, otorgándole o endosándole a nombre propio o de otro, un documento nominativo, a la orden o al portador contra una persona supuesta o que el otorgante sabe que no ha de pagarle;

VII.- Al que vende a dos personas una misma cosa, sea mueble o raíz y recibe el precio de la primera o de la segunda enajenación, de ambas o parte de él, o cualquier otro lucro con perjuicio del primero o del segundo comprador.

VIII.- Al que valiéndose de la ignorancia o de las malas condiciones económicas de una persona, obtenga de ésta ventajas usuarias por medio de contratos o convenios en los cuales se estipulen réditos o lucros superiores a los usuales en el mercado.

IX.- Al que para obtener un lucro indebido, ponga en circulación fichas, tarjetas, planchuelas u otros objetos de cualquier materia como signos convencionales en substitución de la moneda legal;

X.- Al que simulare un contrato, un acto o escrito judicial, con perjuicio de otro o para obtener cualquier beneficio indebido.

XXI.- Al que libre un cheque contra una cuenta bancaria, que sea rechazado por la institución o sociedad nacional de crédito correspondiente, en los términos de la legislación aplicable, por no tener el librador cuenta en la institución o sociedad respectiva o por carecer éste de fondos suficientes para el pago. La certificación relativa a la inexistencia de la cuenta o a la falta de fondos suficientes para el pago, deberá realizarse exclusivamente por personal específicamente autorizado para tal efecto por la institución o sociedad nacional de crédito de que se trate"[9].

Las anteriores concepciones obtenidas del ordenamiento jurídico penal, son las que encuadran a la conducta antisocial a estudiar en este momento, ya que se habla de la utilización de un soporte y de un útil inscriptor, donde se deja en un -pseudo convenio- datos personales, cantidades de dinero y firmas, mismas que son utilizados por personas con intenciones engañosas para obtener un beneficio sea este económico, mueble o inmueble, donde para llevar a cabo esto se realiza una alteración ya sea en una cifra, un grama o una firma.

El delito de falsificación de documentos en general y oficiales, está relacionado con la suplantación de iden-

7 Colectivo Arcion. Dirección General de Investigación 2012.

8 Código penal federal, Publicado en el Diario Oficial de la Federación el 14 de agosto de 1931, ultima reforma publicada en el Diario Oficial de la Federación el 24-10-2011, 'capítulo II Acceso ilícito a los sistemas y equipos de informática, artículo 211 bis' 1. [En línea]. [Consultado: 9 de enero de 2012]. Disponible en la web: http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf

9 Código Penal Federal, Última Reforma DOF 24-10-2011. 'Capítulo lll Fraude' [En línea]. [Consultado: 12 de diciembre de 2011]. Disponible en la web: http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf

tidad, ya que si en algún documento se puede alterar el nombre, la edad, folio entre otros, se podrá obtener otra identidad social y legal.

Otro rubro que no debe pasar por desapercibido es el acceso ilícito a sistemas y equipos de informática, modalidad que también se encuentra relacionada con la suplantación de identidad, por ello es necesario realizar la siguiente apreciación legal respecto a dicha modalidad, objeto que se puede estudiar dentro del Código Penal Federal dentro de los artículos 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6, 211 bis 7 mismos que a la letra dicen:

"Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

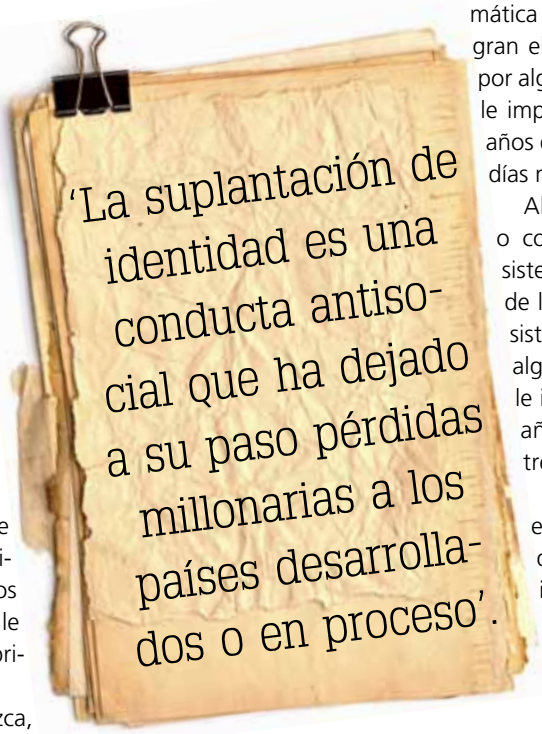
Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando



la información obtenida se utilice en provecho propio o ajeno"[10].

Este es un indicio de lo que sería un delito informático, pero que dentro de esta legislación penal Mexicana se conoce bajo el nombre de Acceso ilícito a sistemas y equipos de informática, donde como se puede observar no se encuentra contemplada la figura de suplantación de identidad, motivo por el cual es necesario reajustar los preceptos jurídicos que se quedan bajo las líneas mientras en la realidad la tecnología facilita la labor del delincuente.

Otro elemento que debe considerarse para introducir dentro de las leyes penales mexicanas la conducta antisocial denominada como suplantación de identidad, es la actual iniciativa que se realizó con base en lo siguiente:

- 300 mil denuncias por robo de identidad con intenciones fraudulentas a bancos y otras instituciones, cifra que ubicó a México en el octavo lugar a nivel mundial en la práctica de esta conducta antisocial.

De éstos argumentos se obtuvo lo siguiente: aprobó en el reciente "periodo ordinario de sesiones"[11] una reforma al artículo 387 del Código Penal Federal, a fin de tipificar el robo de identidad dentro de las figuras de fraude específico, además de que penaliza hasta con 12 años de prisión a quien utilice indebidamente cualquier tipo de identificación, clave de identificación personal bancaria, u otro documento identificatorio que sea de otra persona"[12].

Este proceso se reconoce debido a la falta de conocimiento sobre conductas y su prevención, aunque se tenía conocimiento de que se empezaban a cometer actos ilícitos, por ello "Esta conducta hasta el día de hoy no se había sancionado porque los tipos penales no contemplaban nuevas conductas en las que interviene, inclusive, la delincuencia organizada; es una conducta que anteriormente, por el avance de las tecnologías, no existía"[13].

Existe una falta de análisis desde la óptica de la Criminología-criminalística por parte de las autoridades, ya que no contemplaron la amenaza que otros países manifestaron ante el delito de suplantación de identidad, mismo que iba a vulnerar al gobierno y sociedad mexicana, por ello se hace hincapié en la necesidad de un profesionista que prevea ciertas conductas antisociales que en un futuro generen un problema de mayor consideración.

Suplantación de identidad

La evolución es un proceso que se desarrolla en diferentes circunstancias, una de ellas es la conducta del hombre y la colectividad, este asunto alcanza en ocasiones a crear nuevos delitos, y esto sucede cuando el individuo se da cuenta que ha madurado emocionalmente y ha pasado la línea de superación y de superioridad, luego entonces se da cuenta que es necesario adquirir nuevos conocimientos y artimañas para sobrepasar los límites de lo moral y legalmente permitidos. "La evolución de la criminalidad se presenta en nuevas características para llevar a cabo cierta conducta, dichas características serán aprendidas por unos y mejoradas por otros"[14].

Otro ejemplo de evolución es el despliegue de la tecnología que llega a revolucionar las herramientas de trabajo, es un mecanismo progresivo que perfecciona cualquier actividad, inclusive la seguridad, pero a la par de esta maravilla se encuentran los delincuentes que burlan los sistemas de seguridad de muchas instituciones tanto públicas como privadas, así como la privacidad y confidencialidad de civiles.

Las generaciones de estos años y las futuras, prometen ser muy avanzadas en conocimientos, especialmente dentro de la informática, donde es fácil observar que la población joven manipula a la perfección las tecnologías, todo ello mediante el uso del sistema binario y mediante la exploración, por ello que se ha identificado a sujetos con un coeficiente intelectual promedio que le permite tomar una computadora y llegar demasiado lejos, inclusive hasta ingresar a la base de datos de una institución.

Existen diversas modalidades de efectuar una conducta antisocial, las más comunes van desde el uso de la violencia, hasta idear situaciones que crean engaño, en la primera de ellas, su procedimiento se desarrolla mediante un enfrentamiento a mano armada o usando la fuerza física para dirigirse a la víctima, y cuyo resultado es de manera visible lesiones o en casos extremos causar la muerte, en el segundo de los casos el victimario decide emplear algunas de sus artimañas para obtener algún beneficio ya sea financiero, mueble o inmueble, esto mediante el trato físico frente a frente, donde la víctima es engañada.

A nivel mundial se detectó una problemática de carácter delictivo, donde no necesariamente se violentaba a la víctima, y cuyo ejercicio se desarrollaba únicamente con el empleo de *software* y el uso del internet, su actuación fue desde simples bromas hasta robo de identidad e identidad financiera.

Este fenómeno delictivo se conoce como *'impersonation'* (voz inglesa). Suplantación de identidad. Este término se define de la siguiente manera: "suplantación o identidad a que finge ser una

10 Código Penal Federal, Última Reforma DOF 24-10-2011. 'Título noveno Revelación de secretos y acceso ilícito a sistemas y equipos de informática Capítulo l Revelación de secretos'. [En línea]. [Consultado: 27 de Febrero de 2012]. Disponible en la web: http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf

11 Existen dos tipos de periodos: desiciones ordinarias y desiciones extraordinarias. los primeros son aquellos que se desarrollan en fechas establecidas formalmente. En dichos periodos las Cámaras se ocupan del estudio, discución y votación de las iniciativas que se les presenten y de la resolución de los demás asuntos que le correspondan.

12 Cámara de Diputados, Congreso de la Unión, 'Boletín número 4520'. [En línea]. [Consultado: 3 de enero de 2012]. Disponible en la web: http://www3.diputados.gob.mx/english/005_comunicacion/a_boletines/2011_2011/012_diciembre/18_18/4520_el_robo_de_identidad_origina_en_mexico_perdidas_anuales_por_9_millones_de_dolares_favor_de_utilizar_de_domingo_para_lunes.

13 Cámara de Diputados, Congreso de la Unión, 'Boletín número 4520', [En línea]. [Consultado: 3 de Enero de 2012]. Disponible en la web: http://www3.diputados.gob.mx/english/005_comunicacion/a_boletines/2011_2011/012_diciembre/18_18/4520_el_robo_de_identidad_origina_en_mexico_perdidas_anuales_por_9_millones_de_dolares_favor_de_utilizar_de_domingo_para_lunes.

14 Hikal, Wael. Introducción al estudio de la Criminología, México, Editorial Porrúa, 2011, pág.148.

persona que no es"[15], por solo nombrar algunos casos se conoce la utilización de documentos personales o las tarjetas de crédito y débito.

Tan sólo en América Latina la suplantación de identidad se vislumbra en las siguientes cifras, como se puede observar en la tabla número 1.

TABLA NÚMERO 1
CIFRAS DE ROBO DE IDENTIDAD EN AMÉRICA LATINA

País	Cifra
Ecuador	891 denuncias asociadas al robo de identidad.
Argentina	1700 denuncias de identidades robadas.
Estados Unidos de América	8.4 a 11.1 millones de denuncias de identidades robadas.
México	300 mil denuncias por robo de identidad.

Colectivo ARCION, 12 de enero de 2012. Como se puede observar los países que persiguen esta problemática de manera alarmante son: Ecuador, Argentina, México y Estados Unidos de América, donde éste último es el que presenta cifras más impresionantes.

Es tanta la magnitud de este problema que la Organización de las Naciones Unidas (ONU) ha determinado que esta situación puede llegar a ser una amenaza contra la seguridad de las Naciones.

El robo de identidad, "se ha convertido en la forma más común de fraude al consumidor en Internet, y la manera más corriente es mediante el abuso de información de tarjetas de crédito, esta actividad puede causar efectos depresivos en la economía, elevar los costes del crédito y reducir la confianza en el comercio electrónico"[16].

Este fenómeno creciente es considerado por la misma ONU como una amenaza para la sociedad y que particularmente se perpetra más en países desarrollados con grandes bancos de información y patrimonio financiero.

Para México este tipo de delitos tipificados internacionalmente como robo de identidad es totalmente ajeno, ya que se desconoce la conducta, la magnitud del problema, las dimensiones y las causas que podría tener si no se realiza un estudio a profundidad así como programas donde todo ciudadano de población rural y urbana conozcan el fenómeno y las medidas de prevención que pueden realizar para evitar ser víctima de suplantación de identidad.

Es necesario realizar una apreciación sobre el uso de términos como robo o suplantación de identidad, ya que algunas legislaciones consideran emplear el término de robo al apoderamiento de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley, es decir se habla de una cosa material, siendo esto que puede ser dinero, vehículos, equipos de cómputo, entre otras.

El ser humano no es un objeto material del que se puede disponer, ya que no es una propiedad, o un artículo, por ello se recomienda utilizar una terminología que comprenda no únicamente la modalidad física para apoderarse de una identidad, sino las diferentes formas de expresión delictiva que de ésta se pueda desprender.

Luego de realizar un análisis minucioso sobre la concepción de esta conducta antisocial se llegó a la conclusión de que debiera de utilizarse el término de suplantación, ya que estructuralmente concuerda más con lo que se encuentra desarrollando en la presente investigación.

Por ello se define suplantación como "Acción y efecto de suplantar"[17], y éste último se precisa de la siguiente manera: "Expresión que se define como ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba"[18].

El término -suplantar- contempla dentro de su expresión -al individuo- como dueño de su propia idiosincracia, donde de manera atinada se vislumbra la pérdida de uno de los derechos fundamentales como ciudadano, misma que ha sido disfrutada por alguien más que ocupa los rasgos distintivos ajenos para realizar actividades ilícitas.

Ahora bien la suplantación de identidad se define como "uso indebido de identificaciones personales e información confidencial y privada por medio de vías físicas, informáticas, electrónicas y de telecomunicaciones para ejecutar actividades ilícitas perjudiciales"[19], aspecto que contempla diversas modalidades de la conducta antisocial y no parte únicamente de lo posiblemente tangible.

Es conveniente considerar que muchos de los delincuentes que realizan dicha actividad, mantienen una o varias intenciones delictivas detrás de la obtención de datos personales de sus víctimas, ya que se pueden cometer delitos tales como los que se puede observar dentro del esquema número 1.

15 Cabinas net. 'Robo de identidad'. [En línea]. [Consultado: 12 de enero de 2012]. Disponible en la web: http://www.cabinas.net/informatica/robo-de-identidad.asp

16 ONU 'alerta del robo de la identidad online y el tráfico con pornografía infantil' [En línea]. [Consultado: 13 de enero de 2012]. Disponible en la web: http://www.elmundo.es/elmundo/2010/06/17/navegante/1276776963.html

17 Real Academia Española. Diccionario de la Lengua Española. 'suplantación'. [En línea]. [consultado: 27 de enero de 2012]. Disponible en la web: http://www.rae.es/rae.html

18 Real Academia Española. Diccionario de la Lengua Española. 'suplantar'. [En línea]. [consultado: 27 de enero de 2012]. Disponible en la web: http://www.rae.es/rae.html

19 Colectivo ARCION, Dirección General de Investigación, 07 de febrero 2012.

ESQUEMA NÚMERO 1
ACTIVIDADES ILÍCITAS DETRÁS DE LA SUPLANTACIÓN DE IDENTIDAD

Colectivo ARCION, 22 de febrero de 2012. Estos son tan solo algunos de los delitos que pueden ser derivados de la suplantación de identidad, dicha analogía es tomada con referencia en las legislaciones nacionales e internacionales.

Estos fenómenos se desarrollan ilegalmente de la ayuda de la suplantación de identidad, como ejemplo lo siguiente:

1. Marcos es empleado de una tienda departamental y adquiere un *skimmer* para clonar tarjetas de clientes.
2. Con el dinero obtenido de manera ilícita Marcos adquiere actas de nacimiento falsas donde se observan diferentes nombres de mujeres, hombres y niños.
3. Marcos compra a personas de diferentes partes de la República Mexicana así como de otros países, a las cuales les asigna un nombre y les da un acta de nacimiento que había adquirido.
4. Marcos engaña a las personas que acabo de –comprar-, diciéndoles que van a trabajar en un lugar serio y que les van a pagar muy bien, por lo cual les realiza unos contratos donde estipula algunas condiciones, mismo que es firmado por éstas víctimas, posteriormente Marcos altera cantidades de dinero que eran fruto del trabajo de sus víctimas.
5. Marcos adquiere un pasaporte falso para salir del país y evadir a la justicia.

Suplantación de identidad de tipo físico, informático, y de telecomunicaciones

La suplantación de identidad tiene un sin número de modalidades que son poco perceptibles o desconocidas por la autoridad competente, así como por víctimas, por ello es necesario realizar una clasificación de las modalidades derivadas de ésta conducta antisocial.

De acuerdo a las actividades realizadas por los autores de las conductas antisociales, se conocen tres modalidades y éstas son:

- Físicas. Esta forma se realiza cuando el delincuente realiza actividades mediante el uso de ciertos artificios, con el fin de ocupar el lugar de otra persona.
- Informáticos. Actividad que utiliza métodos, procesos, técnicas y "desarrollos"[20] mediante el uso de ordenadores, con el fin de realizar actividades ilícitas, como el caso de uso de un *software* para modificar la originalidad de un documento de identificación oficial o privada.
- Telecomunicaciones. Uso de otra identidad mediante la utilización de internet o teléfono, para cometer una actividad delictiva.

Dentro de la suplantación de identidad en su modalidad de tipo físico se encuentran las siguientes manifestaciones:

a) Alteración y falsificación de documentos Oficiales y privados, mediante el uso de técnicas como, raspado, borrado, remarcado y anexos. Esta forma es una de las más comunes para su-

20 Desarrollos. Es el conjunto de técnicas y procedimientos que permiten conocer los elementos necesarios para definir un proyecto de software. monografías.com 'Proceso de desarrollo de sofware'. En línea.[consultado: 27 de enero de 2012]. Disponible en la web: http://www.monografias.com/trabajos5/desof/desof.shtlm

plantar a una persona y no necesita de tecnologías o mucho esfuerzo para modificar la originalidad de un documento.

b) Invención de personalidad. Esta es la forma en que una persona pueda crear una carta o constancia de identidad falsa para obtener algún trámite.

c) Robo de documentos a instituciones privadas, o personas. La primera manifestación del robo se empieza a convertir en una situación recurrente, ya que empleados o delincuentes se introducen en la base de datos de instituciones públicas o privadas para obtener información confidencial de ciertas personas, para así poder suplantarla, mientras que la segunda es una forma más cotidiana que es realizada por carteristas que asaltan en camiones del transporte público o transeúntes para obtener información confidencial, ya que toda persona acostumbra a traer entre sus objetos identificaciones personales o claves que muchas veces pueden ser de su cuenta bancaria.

d) Medio de comunicación impresos, como un instrumento para obtener datos personales y suplantar la identidad. Los medios de comunicación impresos suelen ser un instrumento recurrente de los delincuentes, ya que anuncian u ofertan sorteos, premios o trabajos falsos, mismos que logran obtener la atención del lector o víctima, y éstos a su vez realizan acto de presencia al lugar marcado y brindan toda información que se les solicita a tal grado de dejar copias u originales de documentos oficiales.

e) Pepenar documentos que se encuentren dentro de la basura. Esta es una actividad que resulta del descuido de la ciudadanía al dejar todo tipo de información de identificación personal dentro de los botes de basura, acto que es aprovechado por la delincuencia.

f) Suplantación de identidad moral. Esta es una actividad que es realizada por individuos que se hacen pasar por representantes de empresas privadas, para obtener documentos o firmas de víctimas que desconocen la verdadera identidad de los supuestos –funcionarios-, por este medio los delincuentes obtienen información confidencial misma que también puede servir para realizar fraudes.

g) Suplantación de identidad de cadáveres y presos. Esta actividad puede ser completada mediante la información que brindan funcionarios públicos adscritos dentro de un registro civil, Instituto Federal Electoral o Centros de Reinserción Social, ya que son ellos los encargados de realizar un control sobre las defunciones o de ingreso de delincuentes.

Otra forma fácil de realizar es mediante una visita a las tumbas de los cementerios, donde se obtiene el nombre de la persona fallecida que va a ser utilizado para realizar una actividad ilícita.

Delitos Electorales. Esta actividad también está inscrita dentro del código penal federal, donde se prevé que dentro de los artículos 403 y 409.

"Artículo 403 fracción V. Recoja en cualquier tiempo, sin causa prevista por la ley, credenciales para votar de los ciudadanos"[21]. Esta actividad es comúnmente conocida como –"efecto carrusel"[22]-, donde muchas personas con condiciones precarias aceptan –prestar sus credenciales para votar- y recibir a cambio el beneficio que cubra su necesidad momentánea.

"Artículo 409 fracciones:

I.- Proporcione documentos o información falsa al Registro Nacional de Ciudadanos para obtener el documento que acredite la ciudadanía; y

II.- Altere en cualquier forma, sustituya, destruya o haga un uso indebido del documento que acredita

a) la ciudadanía, que en los términos de la ley de la materia, expida el Registro Nacional de Ciudadanos"[23].

Actividad que también se considera como suplantación de identidad, ya que se proporciona información que pueda ser de otra persona o de un finado.

Formas de suplantación de identidad en su modalidad de tipo informático:

a) Clonación de tarjetas. Esta actividad consiste en la "duplicación de tarjetas de crédito o debito sin el consentimiento del dueño de la tarjeta. Los delincuentes que se dedican a esto utilizan diferentes tipos de dispositivos electrónicos que los ayudan a clonar las tarjetas"[24].

b) Alteración y falsificación de documentos mediante el uso de *software*. Es muy común que personas con dominio en la informática utilicen la tecnología para realizar actividades ilícitas, ejemplo de ello la alteración y falsificación de documentos, donde se emplee un *software* que facilite la labor ilícita, como ejemplo de ello el *spy ware*, "programa utilizado dentro de los ordenadores que permite registrar los golpes de las teclas que tocan las víctimas cuando usan su computadora"[25].

Formas de suplantación de identidad en su modalidad de telecomunicación.

Primero se debe definir que es una telecomunicación, y ésta se precisa como toda forma de "comunicación a distancia. La palabra

21 Procuraduría General de la República 'de los delitos electorales' [En línea]. [consultado: 28 de febrero de 2012]. Disponible en la web: http://www.pgr.gob.mx/fepade/cuales%20son%20los%20delitos%20electorales/cuales%20son%20los%20delitos%20electorales.asp

22 Efecto carrusel. Es un sobrenombre que se utiliza para denominar un acto de fraude electoral que algunos ciudadanos realizan, donde organizaciones políticas convencen a la ciudadanía para realizar un voto a favor del candidato político que se encuentran representando a cambio de darles un -beneficio- ya sea éste económico o alimenticio.

23 Código Penal Federal, Última Reforma DOF 24-10-2011, 'Titulo vigesimocuarto, Delitos electorales y en materia de registro nacional de ciudadanos, Capitulo único'. [En línea]. [Consultado: 27 de febrero de 2012]. Disponible en la web: http://www.diputados.gob.mx/LeyesBiblio/pdf/9.pdf

24 Data security.com 'clonación de tarjetas'. [En línea]. [Consultado: 28 de febrero de 2012]. Disponible en la web:http://www.wisedatasecurity.com/clonacion-tarjetas-credito.html

25 Cabeza de Vaca, Daniel F. et al. Intercriminis número 13 segunda época, México, INACIPE, 2005, pág. 311.

incluye el prefijo griego *tele,* que significa -distancia o lejos-. Por lo tanto, la telecomunicación es una técnica que consiste en la transmisión de un mensaje desde un punto hacia otro, usualmente con la característica adicional de ser bidireccional. La telefonía, la radio, la televisión y la transmisión de datos a través de computadoras son parte del sector de las telecomunicaciones"[26].

Cabe mencionar que explícitamente se reconoce el uso de computadoras que permitan la comunicación a distancia, y para ello se requiere del uso del internet, ya que con las redes de comunicación el hombre puede intercambiar conversaciones con gente de otras naciones, o simplemente comunicarse con amigos a través de redes sociales, correo electrónico, o mediante el programa de mensajería instantánea.

La tecnología parecía tan perfecta hasta que el ser humano decidió utilizarla en contra de sus semejantes, por ello que a través de estas herramientas se pueden desarrollar otras actividades que no precisamente son consideradas como benéficas.

Dentro de la magia del internet se pueden realizar actividades de socialización como es el caso de las redes sociales, donde con facilidad hombres y mujeres de cualquier edad entablan conversaciones con gente de cualquier otro lugar del mundo o del país, y en muchas ocasiones el usuario deja al alcance de todos su información confidencial o en situaciones más profundas dentro de la propia conversación acceden a brindar cualquier tipo de datos privados que en muchas de las ocasiones es utilizado por delincuentes que se dedican a suplantar la identidad o contactar a sus víctimas para cometer otros delitos.

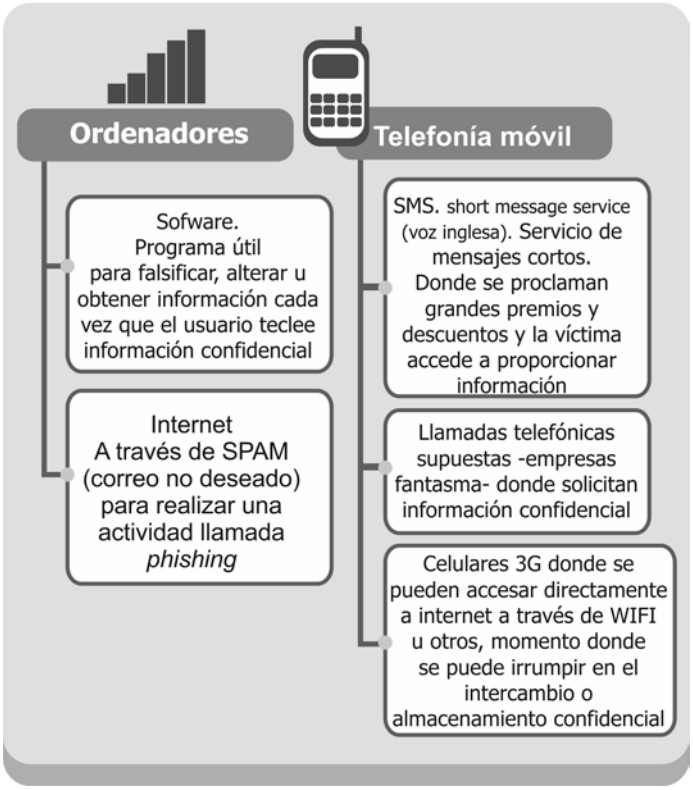
Existe una actividad que está relacionada con el tema que se está desarrollando, y es la simulación de identidad, esta actividad consiste en usar una terminal de un sistema en nombre de otro usuario, y esto resulta por el conocimiento de claves, servirse del abandono de terminales que no han sido desconectadas por el usuario, "El término también es aplicable al uso de tarjetas de crédito o documentos falsos a nombre de otra persona"[27], y esto solo funciona a través de los ordenadores conectados a redes de comunicación.

Otro medio que facilita la labor del delincuente es el llamado –*wifi- wireless lan* (voz inglesa). Red inalámbrica. Esta útil tecnología también sirve al delincuente que realiza un "*hackeo*"[28] a los códigos de los sistemas utilizados por usuarios, ya que dentro de este proceso se pueden realizar intercambios de información, transacciones bancarias entre otras, y es qué gracias a ello, puede ponerse en riesgo la seguridad de la base de datos de las instituciones, con ello se consigue información que puede utilizarse para cometer delitos, y de esta manera suplantar la identidad de quien aún no lo ha descubierto.

Otro fenómeno importante que se desarrolla dentro de ésta modalidad es el llamado –*phishing*- (voz inglesa), pescando. Actividad que se realiza para "obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima"[29].

Esta manifestación vía internet se presenta en las páginas web que son duplicadas, y que muchas veces hacen acto de presencia en los correos electrónicos, donde se encuentran enlaces a sitios web falsos con una apariencia casi idéntica a los sitios legítimos, una vez logrado engaño, la víctima accede ingresar y es justo ahí cuando ingresa sus datos confidenciales como contraseñas, tarjetas de crédito o datos financieros y bancarios, por ello a continuación se muestra el esquema número 2, mismo que describe las desventajas del uso del internet.

ESQUEMA NÚMERO 2
LA DESVENTAJA DE LA TECNOLOGÍA



Colectivo ARCION, 25 de febrero de 2012. Sin lugar a duda la tecnología facilitó la comunicación y la tarea de muchos, pero ésta también es aprovechada al máximo por la delincuencia para lograr obtener la privacidad e identidad de aquellos descuidados y confiados ciudadanos.

26 Definición. de 'Definición de telecomunicación'. [En línea]. [consultado: 29 de Febrero de 2012]. Disponible en la web: http://definicion.de/telecomunicacion/

27 Redel, red de entretenimiento e información. 'Simulación de identidad'. [En línea]. [consultado: 1 de marzo de 2012]. Disponible en la web:http://www.biografica.info/redei/diccionario-de-hacking-25.php

28 Hackeo. Actividad que se realiza mediante la exploración y búsqueda de las limitantes de un código o una máquina.

29 Segu-info seguridad de la información. 'Phishing' [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: http://www.segu-info.com.ar/malware/phishing.htm

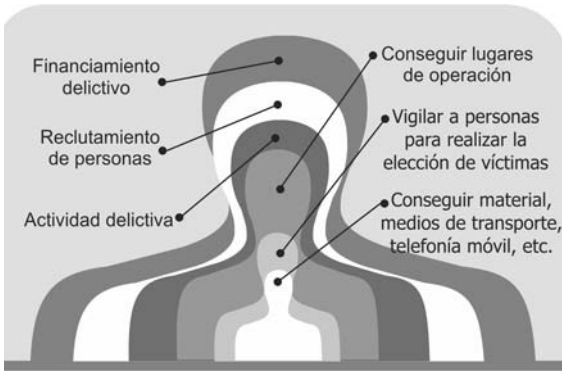
Los grandes problemas de las redes no terminan únicamente ahí, existe una aplicación dispuesta para cualquier dispositivo que utiliza la fuente del internet y es el llamado -*pul wifi*-, este dispositivo obtiene las claves de las conexiones protegidas asignadas por los "routers"[30], esta actividad pone en riesgo la seguridad de las contraseñas de correos electrónicos, tarjetas de crédito, redes sociales y demás que actividades que contemplen información confidencial. Esta es una cara más de la suplantación de identidad en su modalidad de telecomunicación.

Las células criminales y su relación con la suplantación de identidad

Esta conducta antisocial que se desarrolla con potencialidad en la era moderna, toma mayor fuerza cuando grupos perfectamente organizados se dan a la tarea de realizar actividades ilícitas para conseguir grandes beneficios económicos, donde los integrantes pueden llegar a ser profesionistas o gente que sabe manipular los ordenadores, o cualquier otra técnica inmersa para llevar a cabo la suplantación de identidad.

Las actividades que realiza una "célula criminal"[31] están perfectamente coordinadas, se establecen medios, métodos y técnicas para cometer el delito y no verse vulnerado ante las autoridades, es por ello que se convierten en profesionales del delito, por ello dentro del esquema número 3 se muestran las principales actividades.

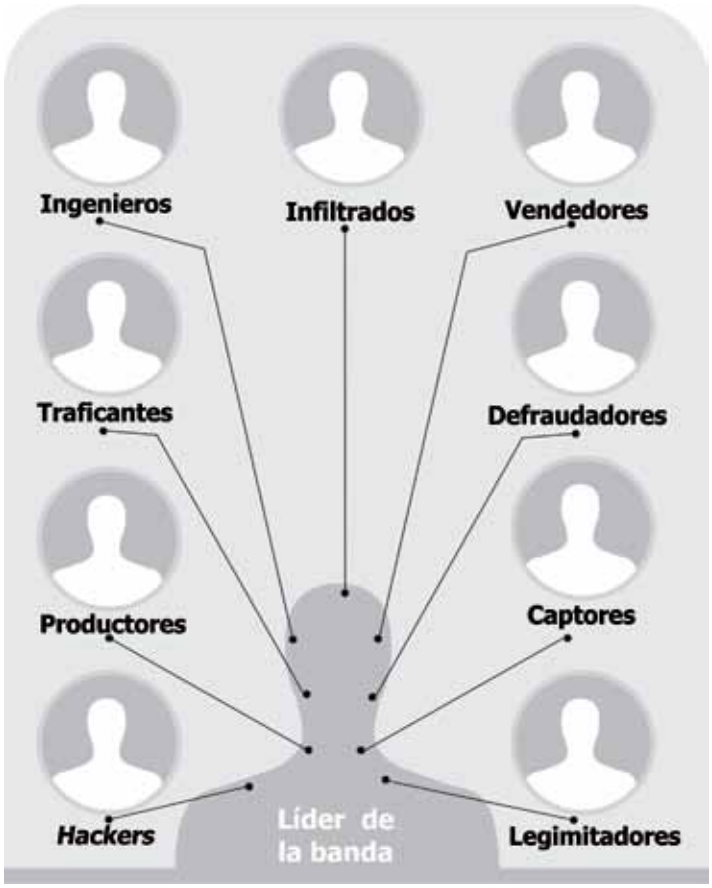
ESQUEMA NÚMERO 3
PRINCIPALES ACTIVIDADES DE UNA CÉLULA DELICTIVA



Colectivo ARCION. 26 de febrero de 2012. Para formar una célula delictiva profesional se requieren de ciertas actividades que la delincuencia requiere para obtener satisfactoriamente sus objetivos.

Estas actividades se encuentran relacionadas con el perfil del delincuente o delincuentes, que son reclutados con base a sus conocimientos o aptitudes, muchos de ellos son profesionistas como contadores, ingenieros, abogados, químicos, administradores, entre otros. De manera paralela también se encuentran aquellos que son contratados por la delincuencia y que solo cubren ciertos requisitos básicos o aptitudes y pueden ser menores de edad, obreros, albañiles, mecánicos, o gente llamada vulgarmente dentro del argot Mexicano como –"ni-ni"[32]-, por ello a continuación se muestra el esquema número 4.

ESQUEMA NÚMERO 4
LOGÍSTICA DENTRO DE LA SUPLANTACIÓN DE IDENTIDAD



Colectivo ARCION, 29 de febrero de 2012. Esquema que muestra la integración de una célula delictiva dedicada a la suplantación de identidad al alimón con algunos delitos.

"*Hackers.* Grupo de personas que penetran dentro de los sistemas informáticos de manera virtual para obtener información confidencial y privada.

30 Un router, (voz inglesa) encaminador, enrutador, direccionador o ruteador. Es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar. Router, Wikipedia, la enciclopedia libre, 'router' [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: http://es.wikipedia.org/wiki/Router

31 Célula criminal. Grupo de personas que funcionan dentro de organizaciones delictivas.

32 Ni-ni. El término de 'ni-ni' hace referencia al sector de la población que en la actualidad no está trabajando ni estudiando (Ni estudia, ni trabaja), siendo la mayoría jóvenes en edad escolar. Los principales detonantes de este problema son la falta de empleo, la deserción escolar y la baja calidad educativa. En Estados Unidos se le conoce a este fenómeno social como NEET (voz inglesa) No employment, no education and no training. Sin empleo, sin educación y sin capacidad. Wikipedia, la enciclopedia libre 'ni-ni' [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: http://es.wikipedia.org/wiki/Ni-Ni

Productores. Grupo de personas dedicadas producir documentos de identificaciones fraudulentas para los traficantes de personas o para realizar otras actividades delictivas derivadas de las identidades de clientes.

Traficantes. Grupo de personas encargadas de "traficar a personas"[33], y tienen completa relación con los falsificadores, ingenieros e infiltrados para obtener documentos oficiales apócrifos y darles una identidad falsa a aquellos inmigrantes, mujeres o niños dentro del territorio nacional.

Ingenieros. Profesionistas en informática encargados de realizar actividades como la falsificación de documentos, realizar actividades como *phishing*, simulación de identidad, clonación de tarjetas, o diseñar programas como *pul wifi* para obtener información confidencial y privada de usuarios del internet.

Infiltrados. Grupo de personas inmiscuidas dentro de instituciones de gobierno o privadas, que se dedican a entrar a la base de datos y obtener información confidencial y personal de trabajadores o usuarios.

Vendedores. Son un conjunto de individuos encargadas de vender datos de información personal o documentos oficiales apócrifos a otras personas que se encuentren en territorio Mexicano que sean indocumentados, que deseen salir del país por evadir a la autoridad, o simplemente para vender dicha información a personas de otros países.

Defraudadores. Son aquellas personas encargadas de engañar a una o varias personas y hacerse pasar por empresas –fantasma- para obtener información confidencial y dinero, otra actividad relacionada con estas personas es la de realizar llamadas telefónicas para engañar a las víctimas y obtener claves bancarias o información personal.

Captores. Grupo de personas encargadas de –echarse un clavado en la basura- para obtener información privada es decir estados de cuenta, copias de identificaciones, claves bancarias, *tickets* de saldos obtenidos de los cajeros automáticos, y demás información que revele la identidad, otra actividad realizada por esta gente es el proceso llamado –búsqueda de túmbas- y ésta consiste en recolectar información sobre personas fallecidas misma que será utilizada posteriormente para hacer creer que él es la persona finada, o simplemente emitir un voto durante el proceso de electoral, es decir la persona que ha fallecido tiene pleno goce de su democracia, procedimiento que se reconoce como una suplantación de identidad de tipo físico.

Legitimadores. Se trata de un conjunto de personas encargadas de realizar una actividad ilícita denominada –lavado de dinero-, su actividad consiste básicamente en canalizar los montos encubriendo los fondos que se hayan generado mediante alguna actividad ilícita como el tráfico de personas"[34].

La necesidad de implementar medidas de seguridad eficaces en el combate contra la suplantación de identidad

En la actualidad, México se encuentra desprotegido ante la conducta antisocial denominada suplantación de identidad, no existe una ley que penalice esta actividad.

Esta forma de expresión criminal es desconocida por las autoridades que día a día se encuentran incapaces ante las demandas que la sociedad exige, ejemplo de ello las tres mil denuncias impuestas ante las autoridades bancarias por clonación de tarjeta, acontecimiento que puso en caos a la ciudadanía y autoridades poblanas, otro caso parecido son los 105 casos detectados por suplantación de identidad dentro de la zona metropolitana y municipios del Estado de Puebla, lo mismo puede estar sucediendo en los demás Estados de la República Mexicana, donde de igual manera queda impune el hecho que se comete directamente sobre la apariencia y patrimonio de la víctima que padece este fenómeno delictivo.

México no se encuentra preparado para combatir la conducta antisocial denominada suplantación de identidad, ya que no cuenta con estudios ni análisis que demuestren la existencia y manifestaciones constantes de este fenómeno, por ello es necesario que los legisladores pongan atención en las denuncias y quejas realizadas por la ciudadanía.

Este procedimiento debe ser analizado y estudiado satisfactoriamente por un Criminólogo-criminalista que identifique las modalidades y los indicios que deja él o los probables responsables y realizar un análisis que muestre:

- Análisis del fenómeno mundial denominado suplantación de identidad.
- Las modalidades de la suplantación de identidad.
- La magnitud del problema.
- El daño ocasionado a las víctimas.
- Probable incremento de la suplantación de identidad.
- Vulnerabilidad de la población.
- Análisis de las zonas donde la población utilice de manera frecuente ordenadores.
- Análisis de los clonadores de tarjetas colocados en los cajeros automáticos de los bancos.
- Análisis de los *skimmer* localizados en tiendas departamentales y negocios.
- Mapeo de la zona para ubicar las zonas donde se hayan reportado clonadores de tarjetas de los cajeros automáticos.
- Mapeo de la zona para ubicar las zonas donde se hayan encontrado *skimmer*.
- Y realizar un programa preventivo que debe darse a conocer a la población en general para evitar ser víctimas de la suplantación de identidad.

Es muy importante resaltar que debe ser cuidadosamente es-

33 La convención de la ONU contra la Delincuencia Organizada y sus Protocolos, definió el Tráfico de Personas, como -el reclutamiento, transporte, encubrimiento o recepción de personas, por medio del uso de amenazas o el uso de la fuerza u otra forma de coacción. Los traficantes son aquellos que transportan emigrantes y se benefician económicamente o de alguna otra manera del de personas-, Un lugar.com 'Tráfico de personas, La tercera actividad ilegal más lucrativa del mundo'. [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: http://www.iuspenalismo.com.ar/doctrina/felipe.htm

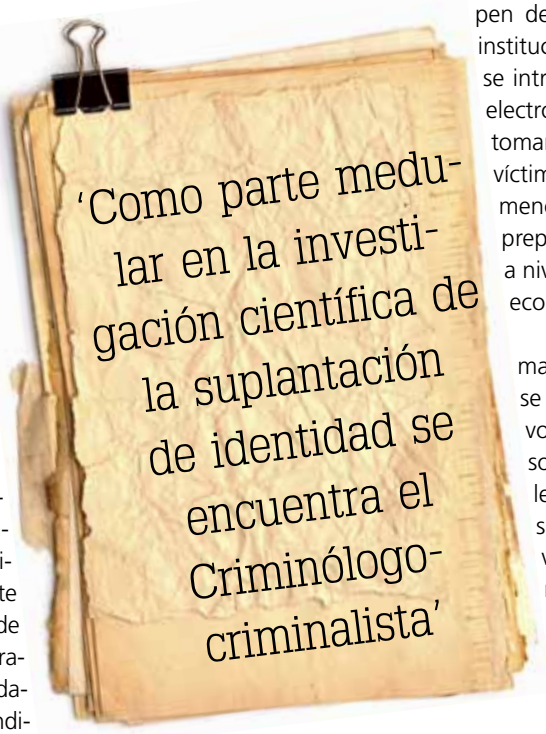
34 Colectivo ARCION. Dirección General de Investigación, febrero de 2012.

tudiado el fenómeno de suplantación de identidad a nivel mundial, ya que de manera indirecta la creación de la tecnología pueden afectar a la seguridad pública e informática de México.

Una vez realizado un análisis profundo sobre la suplantación de identidad por el Criminólogo-criminalista, las autoridades competentes deberán tomar en consideración las demostraciones técnicas y científicas expuestas por el profesionista en cuestión para poder tipificar y sancionar esta conducta antisocial.

Otro factor importante es la prevención terciaria, que se debe desarrollar mediante la implementación de un tratamiento penitenciario adecuado para aquellos sujetos que cometen la actividad conocida como -suplantación de identidad-, ya que si no se atiende al sujeto o sujetos, éstos pueden reincidir en la conducta y hasta mejorar la forma de realizarlo, por ello se debe garantizar el esfuerzo del consejo interdisciplinario para que realicen favorablemente una reinserción social, pero específicamente destacar la labor titánica que deberá de realizar el Criminólogo clínico.

Otro estudio que favorece a la prevención del fenómeno denominado suplantación de identidad es el contacto con la víctima, misma que arrojará datos importantes que ayuden a complementar el análisis realizado por el Criminólogo-criminalista, y finalmente realizar un tratamiento especial de atención víctimas, con todo este trabajo se podrá difundir a la ciudadanía un programa preventivo que indique las acciones que debe tomar para evitar una suplantación de identidad.



CONCLUSIÓN

A través de esta investigación se pudo detectar que el fenómeno delictivo reconocido por otros países como suplantación de identidad tuvo gran impacto, en la sociedad Mexicana, debido a que miles de personas manifestaron sus quejas ante autoridades para pedir justicia ante el hecho de que alguna persona se hizo pasar por ella para dejarlos en banca rota o para conseguir créditos que nunca habían pedido.

Resulta interesante poner atención a los casos de clonación de tarjetas, donde la víctima que padece este fenómeno detecta que le han sido vaciadas sus cuentas bancarias, sin haber hecho ni siquiera un retiro, denuncia que es atendido por algunas autoridades que se quedan incapaces de proceder ante la suplantación de identidad, ya que dentro de los argumentos legales, levemente se consideran iniciativas de ley que contemplan la introducción de dichas conductas en los ordenamientos.

La suplantación de identidad es una nueva conducta antisocial que debe ser estudiada debidamente por un Criminólogo-criminalista, ya que se están pasando por desapercibido muchos factores que son de confort para la delincuencia, y que si no es atendido en estos momentos se puede convertir en un verdadero problema de seguridad que no solo afectaría a la ciudadanía, sino que a la base de datos de las instituciones públicas y privadas.

Esta conducta antisocial que se describe dentro de esta investigación no se manifiesta únicamente de manera física, sino que el delincuente aprovecha la tecnología para cometer sus actividades ilícitas, ejemplo de ello los llamados *hackers* que irrumpen dentro de la base de datos de grandes instituciones de gobierno élite, o simplemente se introduce dentro de las cuentas de correo electrónico de millones de personas que no toman alternativas eficaces para evitar ser víctima de este acontecimiento, dicho fenómeno indica que México no se encuentra preparado para afrontar esta situación que a nivel mundial genera millones de pérdidas económicas.

No solo se trata de identificar el problema o la magnitud de éste, por el contrario se requiere de realizar una opción que favorezca la prevención para disminuirlo, y sobre todo que sea contemplado por los legisladores, para que ellos viertan una sanción oportuna que permita ser aprovechada por el consejo interdisciplinario y especialmente por el Criminólogo clínico que adecuará un tratamiento completo y favorable que facilite la prevención terciaria y evitar reincidencias.

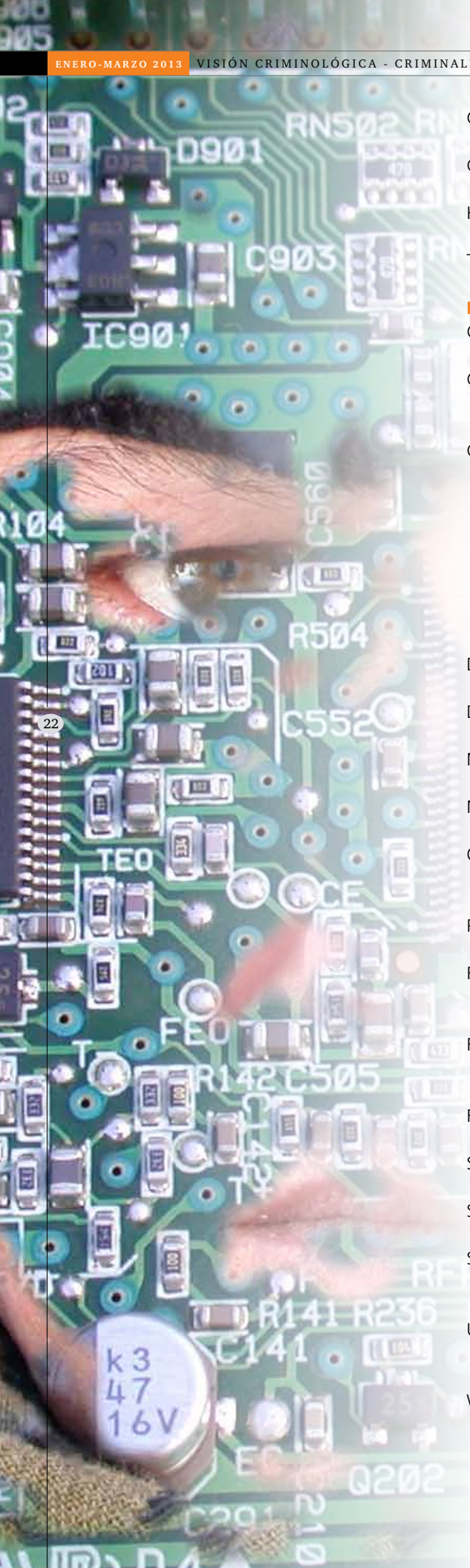
La labor del Criminólogo-criminalista dentro de la llamada suplantación de identidad se encuentra en la detección de nuevas conductas que se ponen de manifiesto mediante el uso material de objetos tales como ordenadores, telefonía celular o *sofware*, es decir mediante el estudio y análisis de la tecnología.

Dichas conductas sirven al investigador científico como base para formular hipótesis que orienten el origen del o de los probables responsables, así como de su conocimiento tecnológico y manejo del mismo, utilizado en contra de la sociedad, todo ello mediante la búsqueda incanzable de indicios materiales que sirvan como orientativos, así como de lo expuesto por la víctima.

FUENTES DE INFORMACIÓN

Bibliográficas

Aboso, Gustavo Eduardo, et al. Cibercriminalidad y derecho penal, Buenos Aires Argentina, Editorial B de F Montevideo- Buenos Aires, 2006.



Cabeza de Vaca, Daniel F. et al. Intercriminis número 13 segunda época, México, INACIPE, 2005.

Cámpoli, Gabriel Andrés. Delitos informáticos en la legislación mexicana, México. INACIPE, 2007.

Hikal, Wael. Introducción al estudio de la Criminología, México, Editorial Porrúa, 2011.

Téllez Valdés, Julio. Derecho informático, México, MacGraw-hill, 2009.

Electrónicas

Cabinas net. 'Robo de identidad'. [En línea]. [Consultado: 12 de enero de 2012]. Disponible en la web: http://www.cabinas.net

Cámara de Diputados, Congreso de la Unión. 'Boletín número 4520', [En línea]. [Consultado: 3 de enero de 2012]. Disponible en la web: http://www3.diputados.gob.mx

Código Penal Federal, Publicado en el Diario Oficial de la Federación el 14 de agosto de 1931, ultima reforma publicada en el Diario Oficial de la Federación el 24-10-2011, 'capítulo II Acceso ilícito a los sistemas y equipos de informática, artículo 211 bis, Titulo noveno Revelación de secretos y acceso ilícito a sistemas y equipos de informática Capitulo l Revelación de secretos, Capítulo lll Fraude, Titulo vigesimocuarto, Delitos electorales y en materia de registro nacional de ciudadanos, Capitulo único' 1. [En línea]. [Consultado: 9 de enero de 2012]. Disponible en la web: http://www.diputados.gob.mx

Data security.com 'clonación de tarjetas'. [En línea]. [Consultado: 28 de febrero de 2012]. Disponible en la web:http://www.wisedatasecurity.com

Definición.DE 'Definición de telecomunicación'. [En línea]. [Consultado: 29 de febrero de 2012]. Disponible en la web: http://definicion.de

Master card 'Robo de identidad'. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: http://www.mastercard.com

Mirrorlinux.net 'hacker'. [En línea]. [Consultado: 09 de enero de 2012]. Disponible en la web: http://mirrorlinux.net

ONU 'alerta del robo de la identidad online y el tráfico con pornografía infantil' [En línea]. [Consultado: 13 de enero de 2012]. Disponible en la web: http://www.elmundo.es

Procuraduría General de la República 'de los delitos electorales' [En línea]. [Consultado: 28 de febrero de 2012]. Disponible en la web: http://www.pgr.gob.mx

Real Academia Española. Diccionario de la Lengua Española. 'suplantación, suplantar'. [En línea]. [Consultado: 27 de enero de 2012]. Disponible en la web: http://www.rae.es/rae.html

Redel, red de entretenimiento e información. 'Simulación de identidad'. [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web:http://www.biografica.info

Router, Wikipedia, la enciclopedia libre, 'router' [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: http://es.wikipedia.org

Scribd. 'Unidad lll. Seguridad informática. [En línea]. [Consultado: 25 de enero de 2012]. Disponible en la web: http://es.scribd.com

Segu–info seguridad de la información. 'Phishing' [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: http://www.segu-info.com

Slideshare present yourself 'Robo de identidad/ identity theft/ Apropiación ilegal de identidad Rivera Suárez, Waleska'. [En línea]. [Consultado: 12 de enero de 2012]. Disponible en la web: http://www.slideshare.net

Un lugar.com 'Tráfico de personas, La tercera actividad ilegal más lucrativa del mundo'. [En línea]. [Consultado: 01 de marzo de 2012]. Disponible en la web: http://www.iuspenalismo.com

Wikipedia, la enciclopedia libre 'Criptología, nini'. [En línea]. [Consultado: 29 de enero de 2012]. Disponible en la web: Criptología http://es.wikipedia.org