Sociologias
ISSN: 1517-4522
revsoc@ufrgs.br
Universidade Federal do Rio Grande do Sul
Brasil

Gabaldón, Luis Gerardo; Pereira, Wílmer
Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico
Sociologias, vol. 10, núm. 20, julio-diciembre, 2008, pp. 164-190
Universidade Federal do Rio Grande do Sul
Porto Alegre, Brasil

DOSSIÊ

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico

LUIS GERARDO GABALDÓN*
WÍLMER PEREIRA**

Resumen

La usurpación de la identidad, entendida como la suplantación del titular de un derecho o crédito por un impostor para obtener un beneficio injusto, recibe cada vez más atención en materia de fraudes cometidos con la ayuda de las tecnologías de la información. Las consecuencias de la suplantación rebasan en muchos casos la pérdida económica directa del titular del derecho afectado, para comprometer su historia crediticia, su prestigio y hasta su identidad social. El artículo discute algunas tendencias en el abordaje legal y en las manifestaciones de los fraudes que implican dicha usurpación, utilizando datos provenientes de una investigación cualitativa en Venezuela, así como los mecanismos de certificación y autenticación que se han propuesto para controlar la verificación de la identidad, destacando sus ventajas y limitaciones. Concluye con una reflexión sobre el equilibrio que debería mantenerse entre mecanismos de seguridad que, multiplicando los controles dificultan la defraudación, y la carga adicional que representa para los usuarios la profusión de los procedimientos de autenticación. en las transacciones electrónicas. Se destaca, finalmente, la necesidad de centrar la atención en la perspectiva de las oportunidades delictivas, que pareciera ofrecer un marco de referencia útil para comprender y minimizar este tipo de defraudación, enfatizando, a su vez, la promoción de iniciativas favorables, en el ámbito de entidades corporativas y usuarios, para la adecuada protección de la información confidencial sensible.

Palabras clave: Certificados digitales. Cifrado. Fraude electrónico. Prevención del delito.

* Profesor Titular de Derecho Penal y Criminología. Universidad Católica Andrés Bello y Universidad de Los Andes, Venezuela. (lgabaldo@ucab.edu.ve)

** Profesor Asociado de Seguridad Computacional y Redes de Computadores, Universidad Católica Andrés Bello y Universidad Simón Bolívar, Venezuela. (wpereira@ucab.edu.ve)

1. El fraude electrónico y la usurpación de la identidad.

En un artículo sobre los fraudes con tarjetas de crédito, Levi (2004:45) identifica cinco modalidades recurrentes: 1) falsificación de tarjetas, cuando se imprimen, embozan, codifican, alteran o recodifican, sin permiso del emisor; 2) fraudes con "tarjetas no presentes", casos en los cuales se suministran códigos o detalles a distancia y a espaldas del titular; 3) fraudes con tarjetas perdidas o sustraídas, que implican su uso presencial mediante el apoderamiento, antes de que el titular reporte la pérdida; 4) fraudes con tarjetas interceptadas antes que lleguen a destino del titular; 5) fraudes por sustitución de identidad, en los cuales un impostor utiliza datos sustraídos o falsos para abrir una cuenta a nombre de otro o utiliza una cuenta usurpada como propia. Las últimas cuatro modalidades implican alguna forma de usurpación de identidad, mediante la cual el defraudador se sustituye o aparenta ser el titular de un derecho de crédito que no tiene, y donde la tarjeta plástica es el soporte material que permite efectuar la defraudación. La primera de las modalidades puede o no implicar usurpación de la identidad, dependiendo de si la cuenta es creada aleatoriamente o se utiliza una cuenta ya existente. Todas las modalidades implican generar un error sobre la identidad del titular, una forma de defraudar que se está extendiendo ampliamente en la era del comercio electrónico.

Una revisión de la literatura reciente sobre el fraude con tecnologías de la información permite observar la creciente preocupación que genera la denominada "usurpación de la identidad" como una modalidad mediante la cual alguien suplanta a alguna otra persona en la titularidad de un derecho o una pretensión para obtener un bien o una prestación. Aunque esta modalidad de defraudación no es novedosa, la difusión de la titularidad de derechos de crédito a través de tarjetas y la extensión del comercio electrónico

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

han planteado, incluso a nivel legislativo, la adopción de tipos legales de incriminación autónoma de esta conducta, así como de otras que pueden ser interpretadas como medios ejecutivos para la usurpación, en particular el denominado *phishing* o pesca a través de la red para obtener información confidencial de titulares de derechos que puede ser utilizada con propósitos de defraudación.

En la literatura anglosajona se distingue entre *hurto y fraude de identidad*, para referirse, en el primer caso a la suplantación de un titular y, en el segundo, a la creación de una identidad ficticia con el fin de defraudar (Lacey y Cuganesan, 2004: 245). Levi (2004: 46) advierte frente al "desliz verbal" que podría implicar la caracterización de la mayor parte de los fraudes como "hurtos de identidad" en cuanto suponen un engaño sobre la verdadera identidad de quien obtiene la consignación, la movilización o la acreditación de la prestación; así, tal engaño se daría tanto cuando se cobra un cheque haciéndose pasar por el beneficiario, haya o no forjamiento documental, como cuando se utiliza una tarjeta de crédito o de débito sustraída o clonada, o cuando se desvía una transferencia electrónica a una cuenta diversa a la cual estaba destinada, sea de persona real o ficticia o cuando se obtiene un crédito bancario mediante el uso de documentación ajena, para citar solo algunos de los casos más conocidos. Por esta razón prefiere utilizar el término de *fraude de solicitud* para los casos en los cuales se utilizan soportes ajenos o forjados para la apertura de cuentas o la obtención de créditos, y el *apoderamiento de cuentas* para la usurpación de tarjetas mediante reenvío, denuncia de extravío y solicitud de reemplazo de la tarjeta extraviada.

El incremento y los costos de las formas delictivas asociadas a la usurpación de la identidad tienden a recibir cada vez mayor atención. Algunas estimaciones para Estados Unidos sugieren que, entre 2002 y 2003, casi diez millones de norteamericanos experimentaron alguna forma de usurpación de identidad, generando pérdidas de 47,6 millardos de dólares para los negocios y de 5 millardos para los usuarios, habiéndose duplicado

la victimización en un periodo de 3 años (Lynch, 2005: 261-262). Se ha determinado que la denuncia de estas conductas es escasa: un 3% de los casos a Comisión Federal de Comercio (FTC) y un 5% a otras agencias (Ibidem, p. 277). Algunos han sugerido que muchas organizaciones de negocios pueden detectar pagos fallidos pero no avanzar hasta determinar si efectivamente hubo usurpación de identidad, con lo cual habría una cantidad de estos casos que quedan sin resolverse, aparte del incentivo que representarían, para la utilización de una identidad suplantada, la presentación de atractivas oportunidades para la compra de bienes y servicios a través de la red (Lacy y Cuganesan, 2004: 256).

Los efectos de la usurpación de identidad rebasan en gran medida las pérdidas patrimoniales directas por las cantidades apropiadas indebidamente, y se extienden a la pérdida o degradación de la capacidad crediticia del afectado, debido a la inclusión en listas de deudores morosos, a la pérdida de respetabilidad e, incluso, a la supuesta participación en diversos delitos cuando la identidad es usurpada. (Lynch,. 2005; Lacy y Cuganesan, 2004).

Un área de vulnerabilidad particular para el uso fraudulento de tarjetas usurpando la identidad está dada por el acceso a bases de datos confidenciales y a computadores personales mediante programas de espionaje (*spyware*). La red se ha convertido en una fuente de alto riesgo para preparar estas formas de defraudación, en sitios donde su uso para adquirir bienes y servicios se ha difundido extensamente y donde no se aplican los debidos controles de autenticación. Estimaciones recientes para Estados Unidos indican que hasta 2/3 partes de las empresas que recogen información sensible sobre clientes no emplean mecanismos de seguridad para salvaguardar los datos, y que hasta el 90% de los usuarios de banda ancha tienen instalado, sin saberlo, algún programa de espionaje para apropiarse de información sensible (Milne, Rohm y Bahl, 2004: 229-230). Por otro lado, entre los usuarios, algunas evaluaciones mediante encuestas sugieren que existe una correlación entre el manifiesto interés en preservar

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

la privacidad, el número de horas de navegación y el nivel de escolaridad, por una parte, y la resistencia a entregar información solicitada en la web y la adopción de algunas precauciones para proteger la privacidad, por la otra (Ibidem: 226). Esto sugiere que las campañas de instrucción y concienciación podrían contribuir a disminuir el riesgo de la suplantación de la identidad de modo fraudulento.

La discusión sobre la usurpación de la identidad en el contexto de un país industrializado con gran volumen de comercio electrónico y donde el control de la capacidad crediticia de los compradores es crucial, guarda relación, como se puede apreciar, con dos hechos conexos pero conceptual y jurídicamente independientes: por una parte la defraudación mediante la obtención de una ganancia injusta a costa de la persona cuyo derecho de crédito se usurpa, y por otro lado, la impostura de la identidad ajena con un propósito más amplio, que incluye pero no se agota en la continuación de la defraudación, como podría ser el evadir responsabilidades penales o el desviar la atención sobre otras actividades ilícitas del impostor. Ello explica la tendencia legislativa a incriminar como delito autónomo la usurpación de la identidad, cualquiera sea la finalidad perseguida con ello (Lynch, 2005).

La extensión del comercio a través de medios electrónicos ha llevado a la creación de nuevos tipos penales que criminalizan la obtención indebida de beneficios utilizando tecnologías de la información, tratando de resolver lagunas de la legislación tradicional en cuanto a quiénes constituyen "víctimas" de la defraudación, titulares de derechos o sujetos en la autenticación de documentos y procesos de pago. Así, la legislación alemana, una de las pioneras en Europa, tipificó la estafa informática como cualquier interferencia en códigos, instrucciones y programas que produce un perjuicio económico mediante la sustitución de la conducta del titular del derecho y no como cesión directa de dicho titular al defraudador, como requería el tipo básico de estafa (Kindhäuser, 2002:665). En la Ley Especial contra Delitos Informáticos de Venezuela (2001) se han previsto como figuras delictivas

independientes el hurto, como apoderamiento de bienes o valores de carácter patrimonial en forma directa (art. 13) y el fraude, como inserción de instrucciones falsas o fraudulentas para obtener el provecho injusto (art.14), distinción que reconoce una conducta directa e inmediata, en el tipo del hurto, y una indirecta y mediata en el de estafa, que pasa por el ardid para inducir la equivocación, en esta última, y que ha sido fuente de disputas doctrinarias y jurisprudenciales. En países donde la defraudación con tecnologías de la información no ha generado una legislación especial, subsisten serias discusiones en torno a la posibilidad de que un computador sea "engañado", dado que conforma un sistema lógico de procesos donde la inducción a error resulta problemática, así como sobre el papel que jugaría el suplantar la identidad de otro para consumar el engaño (Palazzi, 2000: 106-110), lo cual plantea cuestiones vinculadas al delito medio para la obtención de un fin ulterior. Antes de la aprobación de la Ley Especial Contra Delitos Informáticos, la usurpación de identidad era vista como un modo particular de ejecución de la estafa prevista en el art. 464 del C.P. en el caso de fraudes con tarjetas de crédito (Luciani, 2001: 116), aunque después de su promulgación se previeron tipos especiales de defraudación que implican tal usurpación, como la obtención indebida de bienes y servicios sin autorización del titular (art. 15), que implica el uso de tarjetas ajenas haciéndose pasar por su titular, o la alteración de instrumentos electrónicos de crédito o pago con el fin de obtener dichos beneficios (art. 16), que puede operar mediante la réplica de la información en otros instrumentos (clonación) o mediante la incorporación de usuarios a registros informatizados. Si bien la impostura de identidad sigue regulada en Venezuela como delito autónomo por las disposiciones legales relativas a la fe pública, específicamente la falsa atestación (art. 320 C.P.), la legislación especial la ha incorporado como medio de comisión de fraudes en varias disposiciones, aunque no todos los fraudes se ejecutan mediante dicha usurpación.

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

2. Autenticación y certificación de identidad en la era informática.

La multiplicación de las oportunidades de los fraudes a distancia, mediante el uso de la tecnología informática, explica en buena parte que los procesos de autenticación y certificación de identidad reciban creciente atención dentro de este amplio contexto de desarrollo tecnológico. En un trabajo reciente se ha sugerido adoptar un marco de referencia general sobre teoría de la identificación personal para desarrollar una propuesta de control institucional que facilite estos procesos de autenticación. Esta posición asume algunos principios generales (Lopucki, 2001: 97-99): a) La persona que una vez es sujeto pasivo de observación lo será en oportunidades sucesivas; b) La identificación se basa en las características evaluativas o definitorias del sujeto: si ellas coinciden en dos momentos o son lo suficientemente similares o particulares, la identificación resultará positiva; c) La identificación en un nivel (o momento) depende de la fiabilidad del nivel (momento) anterior, y cualquier falla en uno de los niveles afecta al siguiente; d) Los valores característicos deben estar disponibles en los dos lados (o momentos) de la identificación, pues son el criterio de referencia, y por ello no pueden mantenerse en secreto. Estos valores característicos cumplen una doble función: identifican a quien los presenta y prueban que la persona en la segunda observación no está pretendiendo impersonar a otra. De allí surge la importancia de las claves que sólo el titular debería conocer. Esta perspectiva amplia sobre la identificación es aplicable a diversos contexto de cotejo de identidades, desde la inspección visual por aproximación, pasando por la exhibición de documentos, señales características biométricas personales, hasta la exhibición de códigos alfanuméricos de menor o mayor complejidad. Este y otros aspectos sobre verificación de identidad serán presentados con más detalle en la sección 3, infra.

Revisaremos ahora algunos hallazgos y sugerencias sobre las modalidades de fraude en el medio venezolano para sugerir, finalmente, la

consideración de instrumentos de autenticación que refuerzan los procesos de identificación y reducen los riesgos de suplantación de identidades con fines fraudulentos.

3. Defraudación, uso de tarjetas y control de identidad en el medio venezolano.

La información sobre las modalidades, tendencias, facilitadores y respuestas hacia el fraude electrónico en Venezuela es escasa, en parte debido a la novedad de la materia y en parte debido a celos y reservas de organizaciones privadas y agencias gubernamentales. Aunque existe un cuerpo policial nacional con una División Especial de Delincuencia Informática, el acceso a sus registros resulta muy difícil debido a la poca transparencia y al alegado de "reserva de actas de investigación penal", frecuentemente esgrimida cuando se trata de indagar sobre archivos y registros. Existen algunos fiscales del Área Metropolitana de Caracas con competencia bancaria que han sido asignados al manejo de estos casos, pero no hay informes desagregados de sus actuaciones en lo que se refiere a defraudación electrónica. Por ello hemos diseñado un programa de investigación en varias fases que contempla, por una parte, entrevistas y discusiones de grupo con protagonistas de actividades vinculadas a la detección y control de estos hechos y de personas posiblemente vinculadas a la ejecución de algunas formas de defraudación, similar a lo sugerido por Levi (2004), y por la otra, de seguimiento de casos en instituciones bancarias y del sistema de justicia penal. Como era de suponerse, hemos obtenido mejores resultados con la primera estrategia, y a ella nos referiremos para ilustrar el contexto de esta problemática en el medio venezolano.

Una primera aproximación a las modalidades y tendencias del fraude electrónico en Venezuela fue realizada mediante cuatro grupos focales de

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

discusión adelantados entre el 6 de noviembre de 2002 y el 26 de marzo de 2003, con participación de 25 empleados y gerentes bancarios, 5 fiscales o auxiliares del Ministerio Público y 3 funcionarios del Cuerpo de Investigaciones Científicas, Penales y Criminológicas. Allí se pudo observar que el tema de la seguridad y alertas guarda estrecha relación con la utilización de información sensible que se almacena en bases de datos, no suficientemente protegidas, y con la suplantación de la identidad de los titulares de tarjetas de crédito o débito. El tema de la validación de la información contenida en la banda magnética, la información complementaria que se debe requerir antes de aceptar una transacción, bien sea en puntos de venta o a través de Internet, así como la posibilidad de incrementar la información cifrada con tecnología de chip (o tarjetas inteligentes), mereció doce comentarios entre los representantes bancarios en las cuatro sesiones (Gabaldón y Moreno, 2003: 22). La tecnología del chip se sugiere, en este contexto, como un instrumento capaz de recoger, almacenar y devolver información de forma interactiva, lo cual permitiría, fundamentalmente, validar la identidad de quien pretende exhibir la titularidad de la tarjeta, si bien se reconoce que el cambio propuesto podría ser costoso. En cuanto a la generación de claves internas en los bancos para el acceso a bases de datos e información, se reconoce la ventaja del modelo automático de generación de claves, ya que permitiría el cifrado desde el primer momento, cambiando la clave para cada transacción. También se recomendó inducir controles para evitar que personal desincorporado continuase en posesión de claves (Ibidem: 24), lo cual supone un procedimiento de validación de identidad, dirigido no a quien pretende obtener la prestación sino a quien dispone de información que puede ser crucial para autorizarla. Un tema recurrente en la discusión con los trabajadores bancarios es el de los usuarios de las tarjetas reacios a seguir instrucciones sobre su manejo, en particular sobre la delegación de su uso, la suspicacia frente a ofrecimientos de ayuda por parte de terceros y sobre el reconocimiento de la propia tarjeta

una vez que le es devuelta después de efectuar el cargo en un punto de venta (Idem). Los comentarios sugieren que la suplantación de la identidad guarda relación tanto con debilidades tecnológicas como humanas, y que las medidas para minimizarla deberían abarcar varios frentes.

Hemos considerado conveniente, además, escuchar a los protagonistas del fraude, pues se trata de formas delictivas relativamente recientes, donde la innovación puede ser una variable significativa. En este sentido decidimos adelantar entrevistas con informantes privilegiados, esto es, personas que por su experiencia hubiesen estado vinculadas a la defraudación, bien como protagonistas directos o como relacionados cercanos. A tal efecto ubicamos inicialmente a dos personas sugeridas por trabajadores bancarios vinculados a la investigación de los fraudes (solo una de las cuales accedió a ser entrevistada), a fin de generar a través de ellos una muestra tipo "bola de nieve", esto es, de acumulación de personas dispuestas a participar en entrevistas sucesivas. La finalidad es recoger relatos, experiencias y actitudes frente a la defraudación con las tecnologías de la información. Este procedimiento muestral está indicado cuando el universo de los sujetos relevantes es desconocido o de difícil acceso a través de registros convencionales. Entre mayo y diciembre de 2005 pudimos realizar diez de estas entrevistas, de una duración promedio de dos horas, con nueve hombres y una mujer, con edades comprendidas entre 24 y 52 años, quienes han estado vinculados a la comisión directa o al conocimiento estrecho de diversas formas de defraudación, algunas de ellas convencionales, por cuanto sus experiencias se remontan a años atrás, y quienes han relatado episodios e impresiones sobre la frecuencia, modalidades y factores de riesgo de la defraudación en la actualidad.

La cuestión de la suplantación de la identidad surgió de alguna forma en las diez entrevistas realizadas, y en todas ellas tiende a destacarse la facilidad con la cual un individuo puede hacerse pasar por otro, en ausencia de controles de validación de identidad. Aunque existen variados contextos para dichos comentarios, en casi todos se enfatiza en la vulnerabilidad de

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

información confidencial que puede contribuir a victimizar a titulares de cuentas bancarias, mediante uso de tarjetas u otros instrumentos de pago. El cotejo secuencial de la cédula de identidad con la información de la banda magnética replicada es importante para vincular al titular cuya identidad se suplanta con la nueva tarjeta clonada (*Marcos, 15-6-05, p. 2, Charlie, 22-7-05, p. 3)* o se utilizan tarjetas clonadas para consumos en sitios geográficos distantes, donde el control de la identidad del titular es laxo *(Mito, 27-10-05, pp.9-10).* Se utilizan teléfonos hurtados y cuentas *shell* para realizar transferencias fraudulentas ocultando el origen del equipo electrónico y, por consiguiente, la identidad del defraudador (*John, 22-6-05, p. 8)*. Se utilizan programas de computación para acceder a números de tarjeta marcados en sitios de compra *(Benito, 26-10-05, p. 1),* o simplemente se intenta con claves deducidas de documentos fácilmente identificables, como la cédula de identidad *(Rodi, 2-12-05, p. 2).*

En estos comentarios destaca una conducta de apropiación en perjuicio ajeno donde la falla es atribuible a la validación de la identidad de quien realiza la transacción, debido al requerimiento de condiciones mínimas de identificación, como la cédula de identidad, o a la insuficiente protección de la clave, tanto por conservarse una traza física de su utilización o porque la sencillez del código permite fácilmente adivinarla por ensayo o error. Ello sugiere que los mecanismos actualmente disponibles para la validación y la autenticación de la identidad son insuficientes o muy vulnerables.

Dado que la cuestión fundamental entre nosotros constituye la simulación o la adopción de una identidad falsa con el objeto de obtener un provecho injusto, y dado que la limitación de sus efectos puede ser útilmente abordada dentro del marco de una perspectiva situacional y de oportunidades delictivas (Birkbeck, 1984-1985), a continuación proponemos algunos criterios y parámetros que podrían ser considerados para fortalecer los procesos de verificación de identidad y, de este modo, incrementar la

seguridad y reducir la lesividad de la defraudación mediante usurpación de identidad con instrumentos electrónicos.

4. Prevención y seguridad digital: confidencialidad, autenticación y certificados digitales.

La seguridad, desde el punto de vista técnico, se aboca a los mismos desafíos que debe afrontar la seguridad física convencional. Por ejemplo, se debe resguardar el espacio físico de un establecimiento comercial ante el robo de terceros o también, por ejemplo, es necesario que un usuario convencional aplique medidas propias para mantener su integridad personal. En el ámbito digital, hay información que debe ser confidencial y sólo puede ser accedida bajo mecanismos de verificación de identidad del portador. Por ejemplo, es conveniente entregar el número de la tarjeta de crédito a un establecimiento comercial solamente previa verificación de la identidad del ente comercial. Esta constatación de la identidad, denominada también autenticación o autentificación, debe preceder al intercambio de información para asegurar que los datos son entregados y recibidos por las personas o entes autorizados. El reto en la seguridad informática, en el caso de Internet, radica en proceder a la autenticación de usuarios, sin que sea necesario un encuentro personal, para poder transmitir datos confidenciales cuando se realiza una transacción comercial por vía electrónica.

Por ejemplo, un usuario que compra por Internet debe estar seguro de que está interactuando con un sitio de comercio virtual pues, en caso de problemas o fraude informático, debería poder entablar una demanda contra un ente comercial que tenga identidad jurídica. Por otro lado, el establecimiento de comercio virtual debe poder estar seguro que interactúa con el propietario de la tarjeta de crédito para poder cargar la venta de bienes con la debida autorización del propietario.

Usualmente, la manera más utilizada para lograr confidencialidad es el cifrado u ocultamiento de la información, utilizando procedimientos de

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

transformación de los datos. El proceso debe ser reversible a fin de que los entes autorizados o el propietario de la información puedan recuperar los datos originales. Sin embargo, previamente se debe contar con un mecanismo que valide las entidades con derecho para acceder a información confidencial. Para lograr verificar la identidad de una persona existen básicamente cuatro maneras (Garfinkel y Spafford, 2000:105-106):

- Bajo el conocimiento de una secuencia de seguridad o clave,
- Con el porte de un documento o carnet de identificación
- Verificando características propias del usuario mediante aparatos especializados.
- Consultando sobre la ubicación exacta del usuario

El primer método es el más utilizado y se basa en el conocimiento que tiene el usuario de una secuencia de dígitos y/o caracteres para ser autenticado. Se parte del principio de que sólo el propietario conoce esta clave, lo cual permite asegurar su identidad. Sin embargo, presenta el inconveniente de que ante el olvido de la clave el usuario pierde la capacidad de ser autenticado. Además, bajo coacción o descuido un usuario no autorizado puede obtener dicha clave y hacerse pasar por el titular. Este riesgo puede ocurrir aun cuando el propietario tome todas las medidas necesarias, porque para verificar la clave ésta debe estar almacenada en algún repositorio de datos que, desafortunadamente, puede ser accedido por usuarios indebidos o intrusos. Así que un usuario no autorizado puede disponer de la clave si se apropia de la copia que tiene el ente que autentifica al titular. Para agravar esta situación, es común que las personas coloquen claves predecibles o confíen a terceras personas que no resguardan el secreto de la clave en su justa medida.

Debido a estos problemas se ha desarrollado el segundo método, que consiste en exhibir un documento que avala la identidad del portador. Ello se realiza ante un funcionario o aparato capaz de leerlo, lográndose la autenticación sin que el usuario deba recordar ninguna información. No

obstante, se presenta el problema de que sin exhibir el documento el usuario pierde su identidad pues, en realidad, a quien se autoriza es al documento y por ende al portador actual (no necesariamente al propietario). Además está el problema de la falsificación o clonación de documentos, lo cual facilita a personas no autorizadas suplantar la identidad, dado que sólo basta con portar el documento falsificado o sustraído al titular.

Estas deficiencias conducen a un tercer método, más personal, donde el titular no depende ni de una clave que debe recordar ni de un documento que está obligado a exhibir. Aquí se cuenta con un aparato especializado capaz de leer información propia del titular: huella dactilar o palmar, secuencia de ADN, registro del iris, etc. Esta estrategia de autenticación se conoce como biometría y, en principio, resuelve algunas de las deficiencias de los dos primeros métodos. Sin embargo, tampoco es infalible: los dispositivos lectores son aún muy costosos y, desafortunadamente, no son capaces de impedir que bajo coacción un titular sea obligado a exhibir alguna parte de su cuerpo para facilitar el acceso a un intruso.

Por último, está el método de ubicación, generalmente con dispositivos GPS (*Global Positioning System*) que mediante tecnología satelital permite localizar personas en función de la latitud y longitud terrestre (posición respecto al meridiano de Greenwich y al paralelo 0). Esta estrategia ubica con precisión y, bajo ciertas condiciones, se puede saber con certeza la identidad del usuario.

Dado que ninguno de los métodos es infalible, resulta común que se usen combinados para elaborar sistemas de seguridad más robustos y difíciles de violar. Por ejemplo, sistemas de acceso a páginas Web de algunos bancos usan códigos o claves de acceso y además documentos digitales que avalan la identidad del portador. Aunque ambos mecanismos permiten autenticar al propietario de la cuenta bancaria y parecen redundantes, en realidad el objetivo es fortalecer el proceso de verificación de identidad.

Desde el punto de vista técnico, estos cuatro métodos se implantan con programas informáticos que, por ejemplo, solicitan la clave (como es

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

muy común en los cajeros automáticos) o mediante la utilización de carnets con chips o bandas magnéticas (como es posible encontrar en algunas compañías para el acceso a áreas restringidas) o con lectores de registros biométricos (como se usan en compañías transnacionales y, en un futuro cercano, en aeropuertos internacionales).

El método de portar un documento o prenda también se puede emular con un documento digital, no físico, que avala la identidad de su portador. Así, en una transacción electrónica el propietario exhibe un documento digital que permite al receptor constatar la identidad del emisor. Este tipo de documento se conoce como certificado digital. Su finalidad es autenticar ese documento. El documento es auténtico "*cuando el uso del conjunto de datos informáticos que se utilizan como medio para identificar al autor de la declaración haya sido puesto por una persona autorizada y no provenga del abuso del secreto de las claves que lo garantizan* "(Bacigalupo, 2002: 9).

Este documento o certificado digital usa técnicas de cifrado conocidas como algoritmos de clave pública o asimétricos para la autenticación y se apoya en algoritmos de clave simétrica para asegurar la confidencialidad.

4.1. Cifrado simétrico y asimétrico

El cifrado simétrico (Garfinkel y Spafford, 2000: 192-199) se vale de una clave que comparten tanto el emisor como el receptor del mensaje. Así, quien envía la información cifra el mensaje con la clave y el receptor aplica un proceso reverso usando la misma clave para descifrar el mensaje. Estos procedimientos se usan no sólo en transacciones comerciales sino también para el resguardo de información local entre empresas y particulares. Las técnicas actuales de cifrado son muy sólidas y difíciles de romper mediante intentos de encontrar vulnerabilidades en el algoritmo. A pesar de sus múltiples ventajas, el cifrado simétrico adolece, básicamente, de dos inconvenientes:

- Se debe negociar a priori una clave antes del intercambio de información
- Se debe disponer de una clave diferente por cada interlocutor

Ambas condiciones implican serias limitaciones cuando los interlocutores son desconocidos y numerosos. Cuando se intercambia información confidencial con una persona que se conoce personalmente, es relativamente sencillo acordar una clave común que sabemos ambos protegerán. Sin embargo, cuando se interactúa con alguien cuya identidad no puede ser fácilmente establecida, como en el caso de una interacción remota con una agencia bancaria, no es factible el intercambio seguro sin disponer de una clave predeterminada; es necesaria una clave para poder transmitir una clave. Por otro lado, cada vez es más común que todos los sitios comerciales en Internet exijan creación de cuentas personales con claves, lo cual incrementa el volumen de toda esta información y la dificultad para el usuario de resguardarla.

Ante estas limitaciones, en la década de 1980 se consolidó la estrategia de cifrado con algoritmos de clave pública (Garfinkel y Spafford, 2000: 200-202). Estos mecanismos de cifrado ofrecen la posibilidad de autenticar y dar confidencialidad, u obtener ambas cosas. El sistema se fundamenta en que cada interlocutor dispone de dos claves: una privada, que mantiene oculta, y una pública que difunde entre quienes desean comunicarse con él. Si, por ejemplo, Romeo desea enviar un mensaje cifrado a Julieta, aquél cifra con la clave pública de Julieta y ella, al recibir el mensaje cifrado, descifra con su clave privada. Con este mismo par de claves se puede realizar también la autenticación, pues si Romeo quiere hacerle saber a Julieta que se trata de su persona, sólo debe enviarle un saludo cifrado con su clave privada; Julieta, al recibirlo, debe descifrarlo con la clave pública de Romeo y, si recupera el saludo, tendrá la certeza de que quien se comunica con ella es Romeo.

La clave privada se resguarda localmente, cifrándola con algoritmos simétricos y usando otra clave que denominaremos clave de control (en inglés, *passphrase*). Esta clave, conocida sólo por el propietario, oculta la clave privada. En consecuencia, se tiene una información pública que todos deben o pueden conocer (clave pública), que se usa conjuntamente con

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

información secreta bien resguardada por el titular (clave privada), para ofrecer confidencialidad y autenticación.

Los algoritmos de clave asimétrica se usan combinados con los de clave simétrica debido a la lentitud de los primeros y así se logra un mejor rendimiento sobre todo para las transferencias en línea por Internet. La combinación es común en la mayoría de las propuestas de comercio electrónico y transferencias bancarias.

Es claro que para evitar suplantación de identidad algún ente confiable debe avalar las claves públicas, pues por su carácter público o expuesto, ellas pueden ser alteradas. Por ejemplo, un tercero puede generar claves públicas a nombre de otros para suplantar su identidad. Esto conduce a que se debe contar con un mecanismo para avalar las claves públicas, por parte de organismos de comprobada reputación. Estas entidades, también conocidas como Autoridades de Certificación (Verisign Security: 2006), transforman las claves públicas en certificados digitales. Toda la infraestructura que soporta estas técnicas de certificación digital se conoce como PKI (*Private Key Infraestructure*) o Infraestructura Privada de Claves (Garfinkel y Spafford: 2000, 113-119). Así, la mayor parte de las transacciones bancarias y comercio electrónico se sustenta en esta infraestructura para validar la identidad de los entes que participan en un intercambio comercial.

El comercio electrónico exige, al menos, certificado digital para el sitio de venta, aunque no es obligatorio para el comprador. Esto asegura que el cliente tendrá la certeza de que entrega información sensible (su número de la tarjeta de crédito, por ejemplo) a un ente comercial certificado por una Autoridad de Certificación (CA). Algunos bancos venezolanos han intentado implantar el uso del certificado digital del cliente (para autenticarlo frente al oferente del servicio), aunque ello no ha tenido el impacto ni la aceptación deseada. De hecho, la mayoría de los sitios de comercio electrónico no lo solicitan, a fin de facilitar las compras del cliente.

Lo más usual es que los intercambios de compra y venta se realicen usando tarjetas de crédito desde un navegador o *browser*. El navegador

debe conocer de antemano la identidad de las autoridades de certificación para poder constatar la validez de los certificados digitales de los vendedores o de los bancos frente a los clientes.

Finalmente, es claro que la infraestructura PKI es el soporte más utilizado para transacciones bancarias y compra por Internet. En efecto, propuestas como *Cybercash*, *Paypal* o *SET* (*Secure Electronic Transaction*) se apoyan en los certificados digitales y por ende en la PKI, para realizar los pagos con tarjetas de crédito (Asokan et al: 1999). Sin embargo, subyacen en esta infraestructura debilidades que podemos revisar más a fondo.

4.2. Inconveniente de la Infraestructura de Certificados Digitales (PKI).

Independientemente de la propuesta de pago en línea que se utilice: SSL, SET, iKP, *Paypal*, *Cybercash*, (Asokan et al: 1999) o sobre el soporte electrónico bancario, la infraestructura PKI adolece de varias debilidades (Garfinkel y Spafford: 2000, 119-124):

- No está claro si una Autoridad de Certificación (AC) debe ser una institución pública o privada. En caso de ser una empresa con capital privado, los requerimientos de privacidad y confidencialidad de la información de los clientes puede tener un precio (valor de cambio) a ser aprovechado por empleados deshonestos de la empresa, quienes podrían venderla al mejor postor. Por otro lado, en caso de que la Autoridad de Certificación sea una institución pública, los datos de los clientes están sujetos a vaivenes del gobierno de turno y podrían utilizarse con fines no deseados por el usuario, generándose un temor frente al control excesivo del gobierno. Se podría implantar un sistema híbrido donde un ente público regularía a una o varias Autoridades de Certificación que pueden ser públicas o privadas. Sin embargo, por ahora, los entes comerciales y bancarios se certifican mediante AC internacionales.
- La responsabilidad de las AC no es clara en caso de fallas en la infraestructura. De los contratos de acuerdo AC-cliente, también conocidos

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

como CPS (*Certification Practices Statements*), se puede extraer que sólo responden frente a problemas de los algoritmos, los cuales son prácticamente inviolables como lo demuestra la solidez del algoritmo RSA. Además, el usuario está obligado a revisar las lista de revocación, lo cual constituye un procedimiento incómodo y poco práctico (Martz: 2004). Así, es poco probable que estas Autoridades de Certificación pierdan en algún caso una demanda cuando un cliente tenga problemas y sea victima de un fraude en un intercambio comercial (Garfinkel y Spafford: 2000, 129-130).

- Los certificados de cliente, en caso de ser necesarios, deben estar alojados en la máquina local y para que el cliente pueda usarlos en distintos computadores debe transportarlos e instalarlos. Esto puede ser impráctico para personas con poco conocimientos en informática, y aún con la experticia necesaria, constituye un procedimiento tedioso.
- Los certificados digitales, entre sus diversos atributos (tal como lo establece el estándar X509v3) tienen sólo el mínimo de información posible sobre el titular. Apenas su nombre, correo electrónico y dirección. Muchas veces esto no es suficiente para la plena identificación y podría ocurrir que un usuario evada sus responsabilidades contractuales, dado que los escasos datos personales pueden no asegurar una plena identificación.
- El tipo de transacciones que se realiza con la infraestructura PKI desborda el ámbito de los países y los posibles afectados se enfrentarían a una legislación incoherente. Se hace imprescindible contar con una normativa internacional, pero ésta genera controversias y no hay acuerdo en ciertos aspectos fundamentales. Por ejemplo, mientras en los Estados Unidos el carácter probatorio de la firma digital es discutido y pocos estados lo reconocen expresamente (Bradford: 1997), en Venezuela, el Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas (G.O. 37.148, 24-2-2001) establece en el artículo 16: "*La Firma Electrónica que permita vincular al signatario con el mensaje de datos y atribuir autoría a este, tendrá*

la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa." Es fundamental resolver este aspecto y determinar, efectivamente, qué tipo de documentos se pueden firmar digitalmente y cuales no.

Aunque los problemas que presentan los certificados digitales son diversos, hasta ahora ellos constituyen la mejor propuesta para sustentar las transacciones bancarias y comerciales, ya que la biometría no es rentable y aún no muestra una eficacia superior. Este hecho se constata por la preponderancia de las PKI en los intercambios comerciales y el uso muy limitado de la biometría, hasta ahora reducido a ciertos ambientes empresariales.

5. Aplicación de la seguridad digital y control del fraude electrónico.

En la información obtenida a través de los grupos focales de discusión y de las entrevistas con informantes privilegiados, antes mencionados, surgió como tema recurrente la suplantación de identidad en fraudes de uso indebido de tarjetas de crédito y transacciones bancarias no autorizadas. Desafortunadamente esto sucede porque se violentan los mecanismos de autenticación.

Como primera solución pareciera natural la idea de fortalecer la autenticación sobre las tarjetas de crédito y las transacciones bancarias, enfatizando el uso de los certificados digitales y exigiendo claves difíciles de predecir, mediante la adopción de políticas de cambio frecuente. Para ello se requiere de un proceso de concienciación que lleve a los usuarios a valorar la importancia de las claves, quienes personalmente deberían empeñarse en evitar que les sean sustraídas o "adivinadas" por personas no autorizadas. Esto impediría una de las formas más comunes de suplantación de identidad que se reporta, cual es la de aprovecharse de la ingenuidad de los usuarios par obtener la clave.

Las estrategias de protección de las claves deben ser recíprocas, es decir, que los entes comerciales deben apoyar a sus clientes para evitar que

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

les sean sustraídas las claves y ser muy cuidadosos con las copias que poseen, necesarias para la verificación de identidad. Para ello algunos bancos, para evitar la captura de claves con programas maliciosos, obligan al usuario a marcar su clave en un teclado de pantalla sin usar el teclado físico. Además les advierten frecuentemente de no aceptar procedimientos de actualización de datos en línea, ni a través de la página Web ni por correo electrónico. El método fraudulento de captura de información confidencial o *phishing* por página Web se ha sofisticado a tal punto que los portales bancarios ilegítimos son, aun para un usuario precavido, difíciles de detectar. Esto debido a ciertas funcionalidad de Javascript (lenguaje de programación de páginas Web) para modificar la dirección web y así hacer creer al navegador del cliente que está bajando el verdadero portal del banco desde un sitio autorizado (Cross Site Scripting: 2006).

Más aún, los bancos y sitios comerciales también han experimentado con la estrategia de forzar al usuario a cambiar sus claves periódicamente para evitar la sustracción de información confidencial. No obstante, los usuarios, en general, no aceptan fácilmente esta política de cambio, pues los hace propensos al olvido de las claves. Por otro lado, el procedimiento de recuperación y cambio de claves, ante el administrador de la red, es engorroso. De hecho, la mayoría de los administradores obligan al cambio de clave ante olvido, lo cual aumenta el problema de olvido.

También son comunes políticas de longitud mínima de clave y/o bloqueo de cuentas cuando se supera un número máximo de intentos de marcaje de la clave. Estos dos procedimientos han resultado ser muy efectivos y aumentan el nivel de conciencia del usuario sobre la protección de sus claves. Además, limitando el número de intentos al introducir las claves, se evitan los conocidos ataques de fuerza bruta, es decir, atacantes que prueban repetidas veces, generalmente gracias a un diccionario, hasta encontrar la clave. Por ejemplo, es de notar que un pin de tarjetas de débito de 4 cifras permite un máximo de 10.000 combinaciones posibles. Esto implica que,

en el peor de los casos, después de 10.000 intentos, seguro se obtendrá el pin asociado a una tarjeta de débito. Con el límite de solo tres intentos admisibles, la probabilidad de adivinar la clave es muy baja.

En los grupos focales también se manifestó el mal uso de claves por parte de personal deshonesto o desincorporado, accediendo a las bases de datos de los clientes para cometer o permitir fraudes. Sin duda alguna, una política de cambio periódico de claves minimiza el problema, si se conjuga con el uso de claves fraccionadas compartidas; validar el acceso a información confidencial de clientes con claves que deben ser introducidas en el sistema por dos o más empleados disminuye el riesgo de usurpación. Aunque ello produzca procesos más lentos y burocráticos, como compensación se reduce la probabilidad del uso indebido de la información confidencial de los clientes.

Por lo que concierne a las tarjetas de crédito, algunas estrategias de pago en línea, como SSL (*Secure Socket Layer*), obligan al cliente a entregar su número de tarjeta de crédito al vendedor para que éste contacte al banco del cliente y conforme el pago de los bienes adquiridos (Garfinkel y Spafford: 2000, 233-243). El vendedor es el responsable de proteger ese número y evitar que llegue a conocimiento de estafadores y/o clonadores de tarjetas. Ya que la función de un sitio de comercio electrónico no es la seguridad, se han propuesto otros mecanismos automáticos para que el envío del número de la tarjeta de crédito vaya directamente al banco con SET o mediante intermediarios en quienes los bancos confían, como *Paypal* (Asokan et al: 1999). En este caso, la probabilidad de que el número de la tarjeta de crédito sea usurpado por un tercero no autorizado se minimiza, suponiendo que el banco y los intermediarios son confiables. El banco, naturalmente, debería el custodio privilegiado del número de la tarjeta de crédito pues, en caso de fraudes, es justamente quien debe responder ante el cliente.

En los grupos focales también se manifestó el uso de tarjetas inteligentes, valiéndose de la tecnología del chip, para generar mayor seguridad

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

en las transacciones financieras. En Francia, desde la década de 1980, se utiliza un sistema conocido como la *carte bleu*. Inicialmente fue concebida como un plástico utilizable como tarjeta de débito y crédito, tarjeta telefónica y monedero electrónico (Stewart: 2005). Todas estas funciones eran posibles gracias al chip que permitía grabar información y mantener, por ejemplo, el saldo cuando se usaba como tarjeta telefónica. Sin embargo la acumulación de funciones en un sólo instrumento hizo el sistema más apetecible para los delincuentes, requiriéndose, por consiguiente, muchas verificaciones de seguridad, aparte de requerirse de lectores de chips en cada lugar donde el usuario requiriese utilizarlo. En consecuencia, se redujeron sus funciones y se utiliza hoy día con más restricciones. De esta experiencia podemos deducir que el uso del chip en tarjetas de débito y/o crédito es posible si se refuerza con los más recientes mecanismos de seguridad como, por ejemplo, certificados digitales cargados en el chip, lo cual podría ser una opción ventajosa para los bancos.

Sobre esta cuestión podemos destacar que las tarjetas de crédito, a diferencia de las tarjetas de débito, no requieren clave o pin de acceso para cualquier movimiento, sino en aquellos casos en los cuales se pretende adelantos de dinero en un cajero automático. La ausencia de este requerimiento constituye una debilidad desde el punto de vista de la seguridad, aunque una ventaja para el cliente en términos de simplificación del mecanismo de pago. En cierta medida la tarjeta de crédito siempre está activa. Por ello se idearon las tarjetas de crédito virtual o también conocidas como *e-cards*. Con respecto a la seguridad, dichas tarjetas tienen dos ventajas importantes: pueden ser activadas o desactivadas a conveniencia del propietario y no pueden ser clonadas físicamente porque, justamente, son virtuales. Su limitación es que sólo pueden utilizarse para compras por Internet. Sin embargo son un instrumento más seguro que las tarjetas de crédito convencionales para compras e intercambios comerciales electrónicos.

Como ya lo hemos destacado, tanto el uso de claves como de certificados digitales sirven para la autenticación. Usarlos conjuntamente refuerza

los mecanismo de autenticación, pues conocer una clave y poseer un certificado da derecho a acceder a recursos que requieren autorización, para los cuales el cliente ofrece su identidad como aval del intercambio electrónico. Por ello se reduce el riesgo tanto para los operadores financieros como para el propio cliente: mientras más mecanismos de control existan, mayor protección se le brinda al usuario.

6. Conclusiones y Perspectivas

Como se puede apreciar de la discusión precedente, la correcta autenticación se sustenta en el adecuado resguardo de las claves y en el buen uso de los certificados digitales. A pesar de ello, persisten problemas de difícil solución, como los de las personas que comunican claves a terceros por necesidad (en el caso de personas de cierta edad o con impedimentos físicos). Desafortunadamente, cada vez es más común este tipo de fraude sobre personas ancianas o discapacitadas que se ven obligadas a confiar en otros y su solución no es evidente.

Este tipo de problemas o el simple descuido, repercuten negativamente en la efectividad de las claves de acceso, ya que una vez franqueado el proceso de autenticación, no resulta muy complicado para un delincuente realizar un fraude. Cuando la identidad es suplantada, es muy difícil distinguir al verdadero titular del impostor, y sólo se detecta el hecho una vez consumado el delito. Es así como, en el caso de transferencias fraudulentas a terceros a través del portal bancario, ellas resultan posibles cuando el delincuente supera el proceso de autenticación, infracción que sólo será identificada, salvo el caso de alertas parametrizadas, cuando se produzca el reclamo por parte del titular de la cuenta bancaria de origen.

La exigencia de certificados digitales aumenta las barreras que debe sortear un delincuente. Sin embargo, si no se presta la debida atención a la clave de control (*passphrase*) que resguarda la clave privada, también será

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

factible la suplantación de la identidad, dado que el usurpador podrá usar en su beneficio el certificado digital si dispone de la clave privada. Por ello la solución se revierte al adecuado resguardo de las claves. Por otro lado, la garantía que ofrece la confidencialidad pasa completamente a un segundo plano una vez que el delincuente supera la barrera de la autenticación. La confidencialidad no solo no impide el acto de defraudación, que pasa por la vulneración de la verificación de la identidad, sino que, incluso, termina protegiendo al infractor, pues mientras el fraude está en su fase ejecutiva, nadie conoce a favor de quién la información está siendo transferida.

Finalmente, la conocida aseveración de que ningún sistema de seguridad es infalible y sólo hay que implantar uno lo suficientemente difícil de violentar para que el esfuerzo requerido sea superior a los beneficios obtenidos, parece tener plena vigencia en esta materia. Ello implica que el desarrollo de sistemas de protección debe avanzar en torno a la ponderación de los conceptos de valor y magnitud de la oportunidad delictiva (Birkbeck, 1984-85) para equilibrar los costos derivados de la protección del blanco con el desestímulo del incentivo para delinquir.

Impersonation and digital certification: proposals for the control of phishing frauds

Abstract

Identity theft, despite the wider or narrower nature of the concept, is an issue for increasing concern regarding crimes using information technologies, considering its implication both for economic loses and for compromising credit records, prestige and even social identity of the victims. This article discusses some legal and factual trends related to electronic frauds, using qualitative data from a research project in Venezuela to show national tendencies and emerging issues. Certification and authentication processes are discussed along the strength and weakness of different systems, while it is adressed, as well, the balance between multiplying

controls for enhancing safety and overburden of users by applying longer and more demanding processes for authentication and keeping confidential records. A crime opportunity approach is suggested for better understanding modalities and issues related to these type of crime, while promotion of education and responsibility, both at the level of agencies and individuals, is suggested as a useful way for enhancing protection of confidential information.

Keywords: Digital certificates. Encription. Electronic fraud. Crime prevention.

Referencias

ASOKAN N., JASSON P., STEINER M. y WAINER M. **State of the Art in Electronic Payment Systems**, (4 de Octubre de 1999), [en línea], disponible en

http://scholar.google.com/scholar ? h l =en &lr =&q= cache: AMECBKS DJo QJ:www. saunalahti.fi/~asokan/research/ac. ps.gz+link: AMECBKSDJoQJ: scholar.google.com/, [Marzo 2006]

BACIGALUPO Zapatero, Enrique. "Documentos electrónicos y delitos de falsedad documental", **Revista Electrónica de Ciencia Penal y Criminología**, 4, 12, 2002. pp 1-17, en http: //criminet.ugr.es/recpc.

BENCOSME A. y READ P. **Delincuencia Informática**, XIV Congreso Internacional del Consejo Latinoamericano de Estudios de derecho Internacional y Comparado, , Buenos Aires, Abr/2001.

BIRKBECK, Christopher. **El concepto de oportunidades para el delito**: su definición y consecuencias, Revista Cenipec, 9, 1984-1985. pp. 43-81.

BRADFORD, Biddle. Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure, **San Diego Law Review**, Vol. 33, 1997.

Cross Site Scripting, (última revisión 28 de marzo de 2006) [en línea], disponible en http://en.wikipedia.org/wiki/Cross_site_scripting [Marzo 2006].

GABALDÓN, Luis Gerardo y MORENO, María Teresa. **El fraude electrónico en Venezuela**: una aproximación a sus tendencias y modalidades. Informe de la primera fase del proyecto de investigación *Fraude electrónico, lealtad empresarial y cultura corporativa*, Caracas, Universidad Católica Andrés Bello, 2003. pp. 58 (mimeo)

GARFINKEL, Simon y SPAFFORD, Gene. **Seguridad y Comercio en el Web**, México, Mc Graw Hill y O'Reilly, 2000.

Sociologias, Porto Alegre, ano 10, nº 20, jun./dez. 2008, p. 164-190

LACEY, David y CUGANESAN, Suresh. The Role of Organizactions in Identity Theft Response: The Organization-Individual Victim Dynamic, **The Journal of Consumer Affairs**, 38, 2, 2004, pp 244-261.

LEVI, Michael. La organización y regulación comercial del pago fraudulento con tarjetas de crédito, en Luis Gerardo Gabaldón (Coordinador) **Delincuencia Económica y Tecnologías de la Información**. Caracas, Universidad Católica Andrés Bello, 2004. pp. 41-61.

Ley sobre Mensaje de Datos y Firmas Electrónicas, [en línea], 2002, disponible en http://www.sice.oas.org/e-comm/legislation/leyfirmas.asp [Enero 2003]

LOPUCKI, Lynn M. Human Identification Theory and the Identity Theft Problem, **Texas Law Review**, 80, 2001. pp. 89-135.

LUCIANI Gutiérrez, Jorge. La criminalidad informática y la estafa a través de Internet, en Carlos Tablante (ed) **Delitos informáticos: delincuentes sin rostro**, Caracas, En Cambio, 2001. pp. 97-122.

LYNCH, Jennifer. Identity Theft in Cyberspace: crime control methods and their effectiveness in combating phising attacks, **Berkely Technology Law Journal**, 20, 2005. pp. 259-300.

MARTZ, Christine. *CPS - Certification Practice Statement* [en línea], 2004. Disponible en http://www.birds-eye.net/definition/c/cps-certification_practice_statement.shtml,[Marzo 2006].

MILNE, George M., Andrew J. Rohm y Shalini Bahl. Consumer´s protection of online privacy and identity, **The Journal of Consumer Affairs**, 38, 2, 2004. pp 217-232.

PALAZZI, Pablo A. *Delitos informáticos.* Buenos Aires, Ad Hoc. 2000.

STEWART, Doug. **French Property for Sale** [en línea], 2005 disponible en http://www.france-property-and-information.com/Banking.htm, [Marzo 2006].

Recebido: 10/05/07
Aceite final: 03/04/08