

	ARTICULO DEL TRABAJO DE GRADO	Código: F-PI-03
		Versión: 01
		Página 1 de 10

LOS DELITOS INFORMÁTICOS EN EL SECTOR FINANCIERO EN COLOMBIA Y EL HURTO INFORMÁTICO

JULIÁN SANTACRUZ LOAIZA
E-mail: santacruz.182@gmail.com

GAUDI SILVA RUIZ
E-mail: gsilvar_88@hotmail.com

ANTOLÍN ROCA HERRERA
E-mail: antiroca@hotmail.com

Institución Universitaria de Envigado
2017

Resumen: El presente artículo tiene por objeto analizar desde una óptica jurídico-legal los delitos informáticos en el sector financiero en Colombia y el hurto informático; por tanto, a través de un abordaje exploratorio de enfoque cualitativo, se parte de un rastreo bibliográfico y cibergráfico exhaustivo sobre un objeto de estudio relativamente novedoso como es el de los delitos informáticos en el sector bancario conforme a la Ley 1273 de 2009 y su abordaje desde la óptica del tipo penal del hurto. Es por ello que se realizan diversas apreciaciones sobre los delitos informáticos en Colombia y la manera como este se configura en hurto cuando se realiza sobre plataformas propias del sistema financiero.

Palabras claves: *delitos informáticos, Ley 1273 de 2009, sector financiero, seguridad informática, hurto por medio informático, transferencia no consentida.*

Abstract: The purpose of this article is to analyze from a legal-legal perspective computer crimes in the financial sector in Colombia and computer theft; Therefore, through an exploratory approach of a qualitative approach, it starts from an exhaustive bibliographic and cibergráfico tracing about a object of relatively new study as it is the one of the informatic crimes in the banking sector according to Law 1273 of 2009 and its approach From the perspective of the criminal type of theft. That is why various assessments are made on computer crimes in Colombia and the way it is configured in theft when carried out on platforms of the financial system.

Key words: computer crimes, Law 1273 of 2009, financial sector, computer security, computer theft, non-consented transfer.

1. INTRODUCCIÓN

La legislación penal colombiana, a pesar de su extensión, no comprende muchas conductas que hoy en día se deberían considerar como punibles; sin embargo, nuestro Derecho Penal se ha ido actualizando

y acoplado a las nuevas necesidad jurídicas y de justicia que demanda el mundo moderno, donde una de esas necesidades ha sido creada por el desarrollo tecnológico de los últimos tiempos, situación ésta que ha dado lugar a los delitos informáticos como una nueva modalidad delictual.

 <p>INSTITUCIÓN UNIVERSITARIA DE ENVIGADO</p> <p>Ciencia, educación y desarrollo</p>	ARTICULO DEL TRABAJO DE GRADO	Código: F-PI-32
		Versión: 01
		Página 2 de 10

En nuestra sociedad, que se encuentra en constante evolución y más que todo, con el gran cambio que generan los tratados de libre comercio de nuestro país, los delitos informáticos aparecen como un fenómeno de las nuevas generaciones más no ajeno a la nueva legislación que sobreviene; por lo tanto, hay que generar más capacidad de contrarrestarlo e impedir así nuevas formas de perjuicio para las personas, lo que se manifiesta en daños materiales y/o morales.

Por ello en este artículo se abordan los delitos informáticos en el sector financiero en Colombia y la manera como este se configura en el tipo penal de hurtoteniendo para ello presente que la legislación penal colombiana y la legislación internacional, que hoy contemplan diferentes mecanismos para conocer este tipo de situaciones.

Sobre este tema se ve claramente la diferencia en la evolución y el avance de otras legislaciones en otros contextos que contrastan con el bajo desarrollo jurídico y científico de la legislación colombiana sobre el asunto; un ejemplo claro son países como

Chile y Francia que han tipificado este tipo de delitos. Por tal razón, puede resultar algo difícil hablar sobre el tema, debido a la aún poca teoría y estudios que hay sobre la materia.

2. PERSPECTIVAS FINANCIERAS DEL DELITO INFORMÁTICO

Actualmente son las tarjetas de crédito y débito las formas más usadas para la realización de transacciones vía internet. La siguiente forma de pago más utilizada es el cheque digital, el cual funciona como un cheque real, en este caso el usuario utiliza una firma digital que le da validez para más tarde transmitirlo en línea encriptado. Otra forma de pago menos usada es el dinero electrónico:

El término es utilizado en forma general para hacer referencia a una amplia gama de mecanismos de pago utilizados en el comercio electrónico [...]. Estos productos almacenan valores, es decir, registran los fondos o valores disponibles por un usuario del sistema, en un aparato o dispositivo electrónico que se encuentra en su poder (Silva, 2012, p. 8).

	ARTICULO DEL TRABAJO DE GRADO	Código: F-PI-32
		Versión: 01
		Página 3 de 10

Sin embargo, la gran preocupación para empresas y clientes es la seguridad en las transacciones, pero, ¿Qué hace que las transacciones sean seguras?:

De acuerdo con Huayamave (2015), el consumidor encripta los datos de su tarjeta de crédito antes de enviarlos, utilizando programas especialmente diseñados para tal fin, como por ejemplo PGP o el protocolo ‘Secure Sockets Layer’ que se encuentra incorporado al Netscape. La seguridad que proporciona esta tecnología torna casi imposible la interceptación de los datos por un intruso. MasterCard y Visa han adoptado una norma común para el comercio electrónico: SET, *Secure Electronic Transaction*. Esta tecnología intenta superar cinco grandes desafíos: a) garantizar reserva en la información de pedidos y pagos, que se logra por la encriptación de los mensajes; b) asegurar la integridad de todos los datos transmitidos a través de la firma digital; c) verificar que el titular de la tarjeta de crédito sea usuario legítimo de una cuenta, mediante la utilización de la firma digital y los comprobantes de comerciante; d) garantizar la autenticidad del comerciante para que

pueda aceptar pagos con tarjetas bancarias a través de una institución financiera; y, e) facilitar y alentar la interoperatividad entre proveedores de redes y de software.

Al respecto, Gómez (2009) ha manifestado que el riesgo de este tipo de fraudes no depende exclusivamente de la seguridad sobre sus propios sistemas, sino también de la vulnerabilidad que se presenta por prácticas inseguras de los clientes al realizar las transacciones. Al respecto los bancos han venido realizando trabajos importantes en materia de educación al cliente, a través, por ejemplo, de la ejecución de campañas informativas, en las que transmiten mensajes que permiten a los usuarios conocer y aplicar mejores prácticas en la utilización de medios electrónicos para realizar transacciones. De ahí la importancia de la Ley 1273, que impone la aplicación de una pena mayor a aquellas personas que utilicen la tecnología para la comisión de conductas ilícitas. Por un lado, reconoce que su uso facilita consumir algunos delitos y, por otro, que el empleo de medios cibernéticos para fines criminales puede ocasionar efectos en masa e ilimitados.

Por ello, para evitar ser víctima de delitos informáticos, y en especial aquellos de índole transnacional que tienen que ver con el sistema bancario, es necesario “tener presentes recomendaciones de seguridad en las transacciones electrónicas” (Suárez, 2009, p. 68).

Al respecto, Ripoll y Matute (2009) señalan que para el uso de Internet, no se deben realizar operaciones o transacciones en computadores públicos (bibliotecas, centros comerciales, cafés Internet, etc.) o desde computadores desconocidos; para acceder a la página de la entidad financiera, siempre hay que digitar la dirección de Internet; nunca se debe hacer a través de ningún link o enlace; nunca se debe ingresar a la página de la entidad financiera por los enlaces o links que muestren buscadores (google, msn, yahoo, etc); y cuando se realicen transacciones hay que verificar que la dirección de la página donde se pide información confidencial (documento de identidad, números de cuentas, claves, etc.) comience con <https://>

Por correo electrónico, no se debe abrir mensajes enviados por un remitente desconocido; no hacer caso a los correos electrónicos que adviertan sobre problemas en la cuenta o soliciten la verificación o el suministro de información financiera; y no se debe responder estos correos ni hacer clic en ningún enlace que aparezca en el mensaje. Hay que alertar de esta situación a la entidad financiera.

Y a través del sistema de audiorespuesta en teléfonos con pantalla se debe verificar que al marcar la tecla “redial” no quede almacenada la información digitada (número de identificación, de cuenta, clave, los cuatro últimos dígitos de la tarjeta, etc.); se deben realizar las operaciones desde lugares y teléfonos que sean de confianza; y no se deben realizar operaciones marcando números telefónicos desconocidos. No se deben considerar como válidos los mensajes que solicitan llamar a un número.

Hoy en día se pueden realizar transacciones seguras a través de Internet, todo gracias a las medidas de seguridad que las entidades bancarias desarrollan e

	ARTICULO DEL TRABAJO DE GRADO	Código: F-PI-32
		Versión: 01
		Página 5 de 10

implementan constantemente como certificados digitales que evitan la suplantación del sitio en la red, conexiones seguras, encriptación de paquetes, inscripción de cuentas, pago de servicios, topes y registros de operaciones, etc. Sin embargo, siguen ocurriendo fraudes a través de Internet y esto sucede ya que las medidas de seguridad tomadas por los usuarios son deficientes o no existen, pues hay personas que dejan sus datos para validarse en papeles adheridos al computador, grabados en el navegador y utilizan sitios públicos desprovistos de seguridad como algunos café Internet.

3. EL HURTO INFORMÁTICO EN EL SECTOR FINANCIERO

Mediante la tipificación de la conducta del hurto se pretende tutelar la seguridad de la posesión de las cosas muebles. Básicamente es un delito contra el patrimonio económico consagrado en el artículo 239 del Código Penal.

El hurto, según Fernández (2001), tiene por objeto material las cosas muebles e

inmuebles, que sean de naturaleza corporal y en ningún momento incorporeal.

Dentro de los cuestionamientos a la legislación penal el tema concerniente al hurto es fundamental, en especial a la “indiferencia legal” u olvido por parte del legislador de hipótesis como la del hurto a través de medios información.

Para que se configure el delito de hurto en el sector financiero, se necesita que la “cosa” además de ser ajena tenga contenido económico, es decir, no sólo se trata de información financiera, sino también del elemento material y económico que ésta representa.

Sin embargo, este presupuesto producto del análisis de la cosa en el Código Penal no es predicable para el hurto informático. En efecto existen ciertos datos que por su naturaleza tienen índole distinta a la económica, por ello se tutela y protegen con sanciones penales dentro de la Ley 599 de 2000, los derechos de autor.

El derecho penal al referirse al hurto dice que este debe recaer sobre bien mueble ajeno. Esto significa que si la cosa no pertenece a nadie (*res nullius*) o ha sido abandonada, no puede ser objeto material de hurto. Guerrero (2003) considera al respecto, que existe cierto número de informaciones que tienen la característica de *res nullius*.

En efecto, el hurto de dinero, información o programas puede manifestarse de tres maneras distintas. Según Camacho (1987), la primera consistente en que el sujeto activo sustrae el soporte que puede ser en papel o en medio informático y en el que vienen contenidos los datos o programas y como segunda modalidad, el sujeto activo transfiere abusivamente los datos de la memoria del sistema informático, sustrayendo información o valores que se encuentran en documentos informáticos en forma de bits, es decir no apreciables por los sentidos. Aquí efectivamente se concreta el hurto, pero al sustraer el bien no necesariamente se hace mediante su aprehensión material.

Para explicar lo anterior, la doctrina desarrollada por Manzini (1951) se ha basado en la reconocida tesis de quienes han sostenido que la tangibilidad de la cosa no es requisito necesario del sujeto pasivo del hurto.

Para ello asimilan la transferencia de información a circunstancias que se pueden dar, tratándose por ejemplo del hurto de energía eléctrica, gas. No es la acción directa de la mano sobre las cosas objeto del hurto sino es el uso de un medio por el cual la cosa misma pasa indebidamente de una posesión legítima a una ilegítima. De esa forma se concreta el hurto en el sector financiero.

De hecho el hurto informático, puede ser definido como el apoderamiento o sustracción de bienes informáticos de naturaleza mueble con el propósito de obtener un provecho ilícitamente. Al respecto se pueden presentar infracciones tales como: hurto de hardware, software, información de bienes muebles como dineros o mercancías cuando su entrega esté controlado por computador (Hance, 2006, p. 61).

Así mismo se considera importante destacar una forma particular de acceder

abusivamente a un sistema electrónico donde el agente conoce de datos o programas pero no los saca del sistema, es meramente una “aprehensión intelectual abusiva de la información contentiva en un sistema determinado donde no existe norma penal alguna en nuestro ordenamiento” (Ettore, 1998, p. 6).

Se debe considerar que la doctrina italiana así como la francesa advierten que en el llamado acceso no autorizado o abusivo de información no es totalmente acertado hablar de hurto de información por la ausencia de aprehensión material de la información. Se debe aclarar, según Alcívar, Domenech y Ortiz (2016) que el llamado hurto de información en el sector financiero no debe confundirse con hurto de documentos informáticos, que supone que la persona toma un objeto material; que cuando el agente se apropia mediante una operación cognoscitiva de la información contenida en documentos informáticos, accediendo abusivamente al sistema, no es por tanto una conducta que deba calificarse de hurto sino como acceso abusivo.

En lo referente al hurto calificado, es urgente una total modificación, puesto que la expresión usada por el legislador desde el 80, reafirmada por el nuevo estatuto “violando o superando seguridades electrónicas u otras semejantes” no pensó en las verdaderamente novedosas e ingeniosas formas basadas en la electrónica en la magnetización y en la tecnología óptica o magneto óptica que actualmente se ofrece en el mercado y que comunmente utilizan los delincuentes.

Se consideran válidos los argumentos de una buena parte de la doctrina colombiana, en crearse una nueva figura típica paralela al llamado hurto de uso consagrado en el actual Código penal, que podría ser fácilmente apoyada por la doctrina extranjera.

Finalmente es de destacar que frente al hurto informático en el sector financiero quedan importantes retos por afrontar:

No es solamente para las organizaciones o las personas que están en la mira permanente de los ciberdelincuentes. Es un desafío para la sociedad y el Estado, para los jueces y los administradores de justicia, que deben estar preparados no sólo en el conocimiento de la Ley y la

jurisprudencia, sino en el apropiado conocimiento del contexto tecnológico, informático y de sus proyecciones delictivas (Ojeda, Rincón, Arias y Daza, 2010, p. 63).

Sin embargo, al observar las actuales condiciones del sector financiero y su impacto en toda la sociedad, no es exagerado destacar que el reto del cibercrimen, ante las condiciones para enfrentarlo (vistas en el sector tal vez más significativo para observarlo), implican un reto a las propias condiciones de supervivencia y desarrollo de las personas, las organizaciones y las instituciones del país y del mundo.

4. CONCLUSIONES Y RECOMENDACIONES

La doctrina ha sido clara en señalar que los delitos informáticos se han venido desarrollando con el avance de la tecnología y esto hace mucho más complejo poder llegar con los responsables, tanto en Colombia como en otros países estos han tenido mucho más auge, teniendo un impacto en los ciudadanos, afectándolos ya sea económicamente, trayendo consigo responsabilidades enormes en cuanto se

refiere a deudas con las instituciones financieras.

Por el hecho de que una persona siga al pie de la letra todas las indicaciones de seguridad que recomiendan las entidades financieras colombianas, no por ello se encuentra exento de ser objeto de delitos informáticos: desde la clonación de tarjetas de crédito hasta la misma complicidad de funcionarios bancarios pueden dar lugar a que se comenten estos delitos y que, incluso, el cliente puede quedar desprotegido si no dispone de las herramientas probatorias que demuestren su no participación en este tipo de eventualidades.

Resulta bastante llamativo y paradójico que en Colombia las entidades financieras, dentro del cobro que realizan por el manejo por concepto de tarjetas débito y crédito se incluya el pago de un seguro contra hurto, lo cual incluye delitos informáticos; a pesar de ello la entidad no está obligada a devolver el dinero sustraído de una tarjeta débito o crédito.

	ARTICULO DEL TRABAJO DE GRADO	Código: F-PI-32
		Versión: 01
		Página 9 de 10

Se puede afirmar que la modalidad delictiva conocida como delito informático financiero hace tambalear las estructuras jurídicas actuales en el campo del derecho penal, las que no están preparadas para hacerle frente a nuevos hechos sociales por el auge tecnológico.

El tema de informática ha sido una preocupación especial para las entidades del sector financiero; sin embargo, las normas están desarticuladas y desactualizadas en la medida en que el delito informático siempre se encuentra un paso delante de las normas que los persiguen.

REFERENCIAS

- Alcívar T., C., Domenech Á, G., & Ortiz C., K. (2016). La seguridad jurídica frente a los delitos informáticos. *Avances*, 10(12), 41-57.
- Camacho-Losa, Luis (1997). *Delito Informático*. Madrid: Gráficas Cóndor
- Congreso de la República. (2000). *Ley 599, por la cual se expide el Código Penal*. Bogotá: Diario Oficial 44097 del 24 de julio de 2000.
- Congreso de la República. (2009). *Ley 1273, por medio de la cual se modifica el Código Penal, se crea un nuevo bien*

jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Bogotá: Diario Oficial 47.223 de enero 5 de 2009.

- Ettore. G. (1998). *Manual de derecho de la informática*. Buenos Aires: Papel Electrónico.
- Fernández de S., M. (2001). *Atipicidad relativa en los delitos de falsedad, hurto, estafa y daño informáticos*. Santa Marta: Universidad Sergio Arboleda.
- Gómez M., J. (2009). La ley de delitos informáticos: nueva herramienta de protección de la información que impone condenas hasta de diez años. *Semana Económica*, (693), 2-5.
- Guerrero M., M. (2003). *La ciberdelincuencia: la ley patriótica y los efectos globales en las regulaciones nacionales y en particular en el caso colombiano*. Armenia: Universidad del Quindío.
- Hance, O. (2006). *Leyes y Negocios en Internet*. México: McGraw-Hill.
- Huayamave B., X. (2015). La Economía Digital. *Revista Cpymes*, 1(6), 5-19.
- Manzini, V. (1951). *Tratado de derecho procesal penal*. Santiago de Chile: Ediciones Jurídicas Europa-América.

 <p>INSTITUCIÓN UNIVERSITARIA DE ENVIGADO</p> <p>Ciencia, educación y desarrollo</p>	ARTICULO DEL TRABAJO DE GRADO	Código: F-PI-32
		Versión: 01
		Página 10 de 10

Ojeda P., J., Rincón R., F., Arias F., M., & Daza M., L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad*, 11(28), 41-66.

Ripoll B., F., & Matute M., M. (2009). El gobierno colombiano contra los delitos informáticos. *Generación Digital*, 8(1), 49-50.

Silva S., A. (2012). *Delitos informáticos y las TIC*. Carabobo (Venezuela): Universidad de Carabobo (UC).

Suárez S., A. (2009). *La estafa informática*. Bogotá: Editorial Ibáñez.

CURRICULUM VITAE

Julián Santacruz Loaiza: Estudiante de Derecho de la Institución Universitaria de Envigado.

Gaudi Silva: Estudiante de Derecho de la Institución Universitaria de Envigado.

Antolín Roca: Estudiante de Derecho de la Institución Universitaria de Envigado.