



UNIVERSIDAD DE ESPECIALIDADES ESPÍRITU SANTO

FACULTAD DE DERECHO, POLÍTICA Y DESARROLLO

TÍTULO:

DELITOS INFORMÁTICOS COMETIDOS A TRAVÉS DE LOS CAJEROS
AUTOMÁTICOS

TRABAJO DE TITULACIÓN QUE SE PRESENTA COMO REQUISITO
PREVIO A OPTAR EL GRADO DE ABOGADA DE LOS TRIBUNALES Y
JUZGADOS DE LA REPÚBLICA DEL ECUADOR

NOMBRE DEL ESTUDIANTE:

NAYIBE SÁNCHEZ MORENO

NOMBRE DEL TUTOR:

DR. DANIEL KURI GARCÍA

SAMBORONDÓN, AGOSTO, 2019

DEDICATORIA

Este trabajo quiero dedicárselo a Dios mi tío Leonardo, mi bisabuela Aminta quienes me cuidan desde el cielo y en especial quiero dedicárselo a mis padres, Mayra y Xavier, las personas más maravillosas de este mundo.

A ustedes les dedico todo mi esfuerzo, en reconocimiento a todo su sacrificio para que yo pueda tener un mejor futuro y una mejor vida, se merecen esto y mucho más. Quiero que sepan que son mi pilar, que los admiro, que los amo y que les agradezco sus consejos, su preocupación, apoyo y cuidado en cada paso que doy.

A mi mamá, le agradezco que siempre ha estado presente con el abrazo justo en los momentos que más lo he necesitado a lo largo de mi carrera, mi vida y de mi paper de grado, por siempre decirme que me apoya y demostrármelo constantemente con su amor, y por ser la que me motiva a seguir mis sueños no importa el que sea con tal de que yo sea feliz.

A mi papá, le agradezco su constante anhelo y deseo que siempre me vaya bien, por tratar de fabricarme el mejor camino (aunque no el más fácil) para mi desarrollo profesional y personal, por siempre estar dispuesto en altas horas de la madrugada a leer y tratar de explicarme algo que ni yo entendía en su momento y por siempre brindarme su apoyo incondicional.

Les doy gracias por creer y confiar en mí en todo momento, por todo el amor y por hacer de mí con su ejemplo y enseñanzas la persona que soy hoy en día.

AGRADECIMIENTO

En primer lugar quiero agradecer a Dios por ser mi guía, apoyo y fortaleza en momentos de dificultad y de debilidad, por brindarme paciencia y sabiduría para culminar con éxito cada meta propuesta a lo largo de mi vida. De igual manera, quiero agradecer mis padres por ser siempre mi pilar fundamental y haberme apoyado incondicionalmente en cada paso; a mis hermanos Génesis y Xavier por siempre creer en mí y en mis capacidades; a mis abuelas, Natalia de la Torre y Susana Rivera por brindarme en todo momento sus consejos y hombros en los momentos oportunos; y, Gustavo Decker, por darme siempre ánimos para seguir adelante en los momentos en los que más lo he necesitado.

Agradezco a mi Decana, Abg. Alexandra Villacís por apoyarme y brindarme su ayuda en los momentos de dudas y adversidades; a todos los docentes, que con su sabiduría, conocimiento y apoyo me motivaron a desarrollarme como persona y profesional en la Universidad de Especialidades Espíritu Santo; a mi tutor de tesis Abg. Daniel Kuri García, quien con su experiencia, conocimiento y motivación me orientó en el desarrollo de este paper académico; y, Al Econ. Macuy, por sus consejos, enseñanzas, apoyo y sobre todo amistad brindada en los momentos más difíciles de mi vida.

Resumen

En la actualidad, con el avance tecnológico de los sistemas informáticos y de los cajeros automáticos como medio de intercambio monetario entre el usuario y las entidades bancarias, a medida que se avanza con las mejoras para con los usuarios, las organizaciones delictivas están a la par con nuevos mecanismos para apropiarse del patrimonio ajeno por intermedio de alteraciones o usos fraudulentos de tarjetas de crédito y de los cajeros automáticos. En el presente trabajo de investigación, en el cual se analizan delitos pertenecientes al Derecho Informático, desde la legislación ecuatoriana y comparada, se busca identificar plenamente estos delitos, los problemas que ocasionan al sistema judicial y destacar la importancia que tiene la informática para proteger a los usuarios de sufrir perjuicio económico por intermedio de las tarjetas de crédito y cajeros automáticos.

Palabras clave: Derecho Informático, Patrimonio, Perjuicio, Seguridad Informática, Fraudulento, Software, Hardware.

Abstract

Today, with the technological advancement of computer systems and the atm machines as a means of monetary exchange between the user and the banking entities as it moves forward with improvements for the users, the criminal organizations have plenty of knowledge about the new mechanisms for appropriating the patrimony outside through alterations or fraudulent use of credit cards and atms. In the present research work, which looks at crimes belonging to the Computer Law, considering the ecuadorian legislation and comparative, are looking to fully identify these crimes, the problems caused against the judicial system and to highlight the importance of technology information to protect the users suffer economic loss through credit cards and atms.

Key words: Computer Law, Patrimony, Harm, Informatic Security, Fraudulent, Software, Hardware

I.- Introducción

El propósito de esta investigación es analizar el impacto que poseen las nuevas tecnologías y el estudio que tienen los infractores en esta clase de delitos informáticos. Estos infractores, utilizan sus conocimientos en temas de tecnología para aprovecharse las vulnerabilidades que existen en los sistemas informáticos de los cajeros automáticos y en la elaboración de tarjetas de crédito; debido a esto se pueden lograr su cometido, el cual es beneficiarse a gran escala del patrimonio de terceros. A su vez, se busca posterior a la identificación de los problemas que tienen los cajeros automáticos, a proponer soluciones que de forma preventiva puedan evitar el cometimiento de estos delitos, o en su defecto, una vez consumados, tener las herramientas necesarias en la investigación penal para ubicar a los infractores y que puedan ser sujetos a un debido proceso, en base a pruebas que muestren la responsabilidad penal. En lenguaje simple, podemos entender como delito informático a toda conducta típica que vulnere derechos de un tercero, en la que se utilice a la computadora como instrumento, medio o fin¹.

El problema radica en el caso concreto de la estafa mediante cajeros automáticos, en que no es fácil determinar con exactitud al infractor o los infractores, dado a los mecanismos tecnológicos o de software que se pudieran cometer, además no es común que el sujeto activo cometa directamente la infracción en calidad de autor. Por ello, hay un postulado muy interesante y de utilidad para entender la naturaleza de los delitos que se van a analizar, el cual el uso de computadoras se manifiesta de diferentes maneras: en la primera, el ordenador puede ser el objeto de la ofensa; en la segunda, la computadora puede ser la herramienta del delito y finalmente, las computadoras resultan incidentales en los delitos, en la medida que contienen evidencias de estos². Lo importante de este postulado es que podemos a breves rasgos apreciar el uso que tiene la computadora, y actualmente, los sistemas informáticos y conocimiento de los

¹ VIZUETA RONQUILLO Juan, *Delitos Informáticos en el Ecuador*, Editorial Edino, Guayaquil, 2011. P

² REYNA ALFARO Luis Miguel, *Los Delitos Informáticos*, Justita Editores, Madrid, 2002.

infractores, para cometer ilícitos, y como se verá, los delitos de los cuales los cajeros automáticos y tarjetas de crédito son vulnerables.

II.- Problemática de las estafas mediante cajeros automáticos

Es pertinente indicar que la problemática de los delitos a través de cajeros automáticos tiene tal relevancia en la sociedad ecuatoriana y mundial dado que a través del sistema informático (*hardware* y *software*) se pueden perpetrar una serie de delitos. Partiendo de una tipología no exhaustiva de conductas vinculadas con la tarjeta bancaria, se podrían señalar las siguientes: falsificación de tarjeta bancaria, colocación de instrumentos electrónicos en cajeros automáticos que descifren los datos de tarjetas bancarias para su clonación, falsificación del documento que convierte al sujeto en titular de una tarjeta auténtica, falsificación de la firma que incorpora una tarjeta auténtica, uso ilícito de una tarjeta obtenida de forma legal, uso ilícito de una tarjeta falsificada, uso ilícito de una tarjeta ajena obtenida a través de un delito patrimonial, uso ilícito de una tarjeta obtenida a través de engaño realizado al emisor, uso de los datos de una tarjeta de crédito o débito a través de Internet, entre otros³. Para impedir la realización de estos delitos, como medida preventiva, es necesario contar con la seguridad informática que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar a menoscabos contra la información⁴.

El *modus operandi* en este tipo de delitos de los cuales los cajeros automáticos y las tarjetas de crédito son susceptibles, es en muchos casos complicado de determinar con exactitud, dado que los delincuentes tienen a la mano varias posibilidades de acción para ejecutar estos delitos, además de que se caracterizan que con el avance de la tecnología, estos sean más sofisticados y al mismo tiempo protegen la identidad y ubicación de quien adecúa su conducta en el tipo penal correspondiente. Estos delitos tienen la particularidad de que terminan en la consumación de la estafa, que es muy común que sean realizados tanto en el lugar donde se ocasiona el agravio a la víctima como en otros países,

³ RUIZ LUÍS RAMÓN, *Uso Ilícito y Falsificación de Tarjetas Bancarias*, Revista de Internet, Derecho y Política UOC, Barcelona, 2013.

⁴ ÁLVARO GÓMEZ VIEITES, *Enciclopedia de la Seguridad Informática 2da Edición*, Editorial Alfaomega, Ciudad de México.

dando además más formas de cooperación criminal en calidad de autores y cómplices.

En el caso de instituciones financieras, estas vienen realizando inversiones en tecnología, pero no son suficientes en la medida en que se desarrollan procesos capaces de vulnerar los sistemas más complejos utilizados por los bancos, tomando estas organizaciones delictivas la delantera o estando a la par tecnológicamente hablando. La mayor parte de los delitos informáticos denunciados han sido registrados como falsificación o estafa, tal como se muestra a continuación: Las denuncias receptadas en Guayaquil entre el 1 de enero y el 25 de abril del 2010, en la modalidad de delito con tarjetas bancarias fue de 66, 67 % y con transferencias bancarias de 33,33 %. A nivel de daños informáticos ha habido 249 denuncias con apenas 2 instrucciones fiscales, en falsificaciones electrónicas ha habido 23 noticias de delito con solo 1 instrucción fiscal, en apropiación ilícita por medios informáticos se han denunciado 168 casos en los cuales existió 13 instrucciones fiscales⁵.

Como antecedente, es llamativo ver la poca continuidad procesal que han tenido estos delitos en la provincia del Guayas, con lo que podemos obtener las siguientes conclusiones: es evidente la importancia del cuidado que merecen las tarjetas de crédito y su protección, tanto por parte de los usuarios como de las entidades financieras, y el debido conocimiento que deben tener los jueces, peritos y fiscales al momento de conocer los delitos que éstas acarrearán dado su relevancia económica y lo difícil que puede ser rastrear al delincuente. El engaño y manipulación informática se presentan en principio como dos conductas delictivas nítidamente diferenciables, lo que determinará que también difieran los cursos causales que deberán unirlos con el perjuicio patrimonial ajeno, para completar los injustos correspondientes a cada uno de estos delitos⁶.

Ahora bien, las estadísticas en la actualidad son bastante impactantes por cuanto el avance de la tecnología sigue en auge, continúan nuevas y más sofisticadas modalidades de delitos informáticos que tienen a cajeros automáticos

⁵ VIZUETA RONQUILLO Juan, 2011, P.112.

⁶ GONZÁLEZ CHUSCA & VIVES ANTÓN, *La Estafa Informática*, Editorial Ibáñez, Madrid, 2006.

y demás equipos informáticos como medio. En el 2017 se investigaron 530 casos de delitos informáticos, en la provincia del Guayas se registraron 18 casos; en la provincia de Pichincha 145, en la provincia de Manabí 24, en El Oro 22, según las fiscalías provinciales de cada una de estas provincias. Un dato que llama mucho la atención, dado a la facilidad que tiene el delincuente de estos delitos, es dificultar el rastreo de las autoridades, porque estos delitos pueden ser cometidos desde cualquier parte del mundo, tal es así que China, Estados Unidos y Brasil son los países de donde proviene la mayor cantidad de ataques cibernéticos⁷.

Las prácticas habituales para llevar a cabo del delito o fraude en cajeros automáticos, se pueden catalogar de cuatro maneras distintas según sus características. La primera es la trampa de tarjeta que consiste en la obtención de la tarjeta física original junto al código secreto o PIN, para llevar a cabo este tipo concreto son habituales el uso de cambiar los teclados de los cajeros para obtener dicho código y un posterior atraco para la tarjeta. También podemos encontrar otra categoría de fraude en los cajeros automáticos que se denomina Clonación de tarjeta y se caracteriza por la obtención del código secreto y los datos de las bandas magnéticas de la tarjeta. Para conseguir estos datos se suele recurrir a dispositivos falsos colocados en el cajero automático⁸.

El *cloning* o *skimming* constituye una forma delictiva por la que se duplican tarjetas de crédito o débito sin que sean sustraídas de sus titulares, valiéndose de empleados de restaurantes, tiendas, y otros lugares públicos, a quienes los autores les proveen de pequeños artefactos electrónicos para copiar toda la información de la banda magnética; incluso se ha llegado a descubrir el uso de franjas lectoras de datos en las ranuras de cajeros⁹. Esta modalidad sin duda acapara mucha de la atención de las autoridades, usuarios de tarjetas de crédito y por supuesto, de los delincuentes que aprovechan los avances tecnológicos y descuidos de los usuarios de tarjetas para que con un pequeño

⁷ EGRED Joan Paul, Redacción Justicia, Diario El Telégrafo, Quito, 2019.

⁸ COPMAN SPECTOR Sebastián, *El Delito de Estafa y los Nuevos Medos de Pago*, UOC, Barcelona, 2015.

⁹ JAÉN VALLEJO Juan, *Cuestiones Actuales del Derecho Penal Económico*, Editorial Ad-Hoc, Madrid, 2004.

artefacto capaz de copiar información valiosa y sensible de las tarjetas de crédito, puedan usarlas fraudulentamente a su favor.

Por último se encuentra otro tipo de fraude no tan sofisticado conocido como trampa del efectivo que se distingue por la utilización de mecanismos rudimentarios que se colocan en la boquilla dispensadora de billetes del cajero en cuestión con la finalidad de ocultar e impedir que salga el dinero de la víctima. Usualmente los delincuentes que llevan estos delitos a la práctica, no son delincuentes cualesquiera sino que son concedores y expertos de la práctica, además suele llevarse a cabo entre grupos de delincuentes organizados¹⁰.

III.- Tipificación del delito en el Ecuador

Previo al análisis de la norma jurídica que el legislador ha optado por incluir en el Código Orgánico Integral Penal, los delitos informáticos enfocados a los cajeros automáticos y tarjetas de crédito comparten dentro del tipo objetivo la acción que tipifica la ley como delito. Para el sujeto activo, se trata de la persona que realiza la conducta tipificada en la ley, entre quienes pueden ejecutar los ilícitos podemos mencionar. El sujeto pasivo es la persona que sufre el ataque informático y los delitos conexos que se analizan en este trabajo de investigación. El uso fraudulento por terceros no autorizados es el principal problema que presenta el funcionamiento de la tarjeta de crédito. La apropiación de ésta por personas extrañas y su utilización ilegítima ocasionan daños a uno o más de los sujetos participantes del sistema de tarjetas de crédito (usuarios, establecimientos adheridos, entidades emisoras)¹¹.

Sobre la interceptación ilegal de datos, en Colombia el artículo 269 C del Código Penal Colombiano menciona que este delito al igual que en Ecuador, es punible en el momento es que se comete sin previa orden judicial, interceptando datos informáticos dentro de un sistema informático o emisiones electromagnéticas provenientes de un sistema informático, será penado con pena

¹⁰ JAVATO MARTÍN Antonio, *Las Tarjetas de Crédito y Débito (aspectos penales)*, Universidad de Salamanca, 2013.

¹¹ MARIÑO LÓPEZ Andrés, *Uso Fraudulento de Tarjetas de Crédito por Terceros no Autorizados*, Editorial Marcial Pons, Madrid, 2006.

de prisión¹². Es muy parecido entonces este artículo al establecido en el 230 del COIP, que para efectos prácticos, tienen los mismos elementos constitutivos que a su vez son de mucha ayuda en caso de que estos países requieran asistencia mutua.

Comparando el delito de producción, tenencia y tráfico de instrumentos destinados a la falsificación de moneda en el COIP, resulta difícil encontrar en países latinoamericanos o europeos este tipo de delito, lo cual implica un adelanto jurídico que tiene el Ecuador al momento de haber expedido el COIP, porque con esto se busca prevenir el cometimiento del delito de falsificación de moneda, además de sancionar la mera tenencia de estos materiales, siendo un delito de peligro. Sin embargo, en el Código Penal chileno encontramos en el artículo 167 que menciona que el que de concierto con los falsificadores o cercenadores, tomare parte en la emisión o introducción a la República de la moneda falsificada o cercenada, será castigado con las mismas penas que por la falsificación o cercenamiento corresponderían a aquéllos según los artículos anteriores¹³. Este artículo tiene una gran aproximación con el 305 del COIP ecuatoriano, porque se penaliza a quienes faciliten la labor de los falsificadores, para lo cual se puede subsumir el comportamiento de asistir con materiales, conocimientos y demás herramientas para la falsificación de moneda, sea esta en billetes o monedas, tarjetas de crédito y demás títulos de crédito.

De la falsificación de moneda, el Código Penal peruano en su artículo 252 explica que el que falsifica billetes o monedas será reprimido con pena privativa de libertad. El que falsifica billetes o monedas separando el anverso y el reverso de los auténticos, superponiendo sus fragmentos, recurriendo al empleo de disolventes químicos, usando los fabricados por otros países, recurriendo a aleaciones distintas o valiéndose de cualquier otro medio que no fuere de producción masiva, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de diez años y con ciento veinte a trescientos días más multa¹⁴. Vemos que a diferencia con el COIP, el COIP incluye como modalidad de

¹² CÓDIGO PENAL COLOMBIANO (Ley 599 del 2000 actualizada), Bogotá, 2000.

¹³ CÓDIGO PENAL DE CHILE, Ministerio de Justicia, Santiago, última actualización. 2011.

¹⁴ CÓDIGO PENAL DE LA REPÚBLICA DEL PERÚ, Ministerio de Justicia, versión actualizada al 16 de octubre 2018, Lima.

falsificación los medios de tarjetas de crédito, ya que es un título de crédito monetario susceptible de este delito.

En lo relativo a la estafa, el código penal español en su artículo 248 estipula que en los elementos subjetivos del delito son el ánimo de lucro e inducir al error en el otro, un acto por el cual la víctima disponga de su patrimonio en beneficio del infractor. Es llamativa la paridad en legislación con el Ecuador y España, considerando que los literales B y C de este artículo contienen lo siguiente: Literal B, Los que fabricaren, introdujeran, poseyeran o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo. Literal C, Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero¹⁵.

Finalmente, es indiscutible que el orden en el cual estos delitos han sido estudiados bajo el marco jurídico de varios países de habla hispana, denota el parentesco que hay en materia de imputación objetiva, porque los sujetos activos y pasivos estos delitos son los mismos, además del bien jurídico protegido que radica en los mismos. Se entiende que hay algún tipo de manipulación informática, cuando se alteran los datos con que opera el sistema informático, sea por introducir datos falsos o por ocultar los verdaderos. Pero, por realizar una operación comercial mediante el uso del número de tarjeta de crédito, obtenido de manera fraudulenta, no se considera que se produzca una manipulación informática, sino solo que se ha dado un uso fraudulento a la tarjeta de crédito en particular. Cabe hablar también como una forma de manipulación informática, la obtención de dinero sobre la base de la alteración de los datos contenidos tales como: datos del titular, entidad, cuenta bancaria, número de identificación (PIN) y monto diario disponible en la banda magnética de la tarjeta¹⁶. Como se aprecia, se comparten los mismos preceptos de estos literales que agravan el delito de estafa, por razón de que para su cometimiento, es evidente la premeditación de infringir la norma penal con conocimientos necesarios para lograr este delito que si bien es

¹⁵ CÓDIGO PENAL ESPAÑOL & LEGISLACIÓN COMPLEMENTARIA, Ministerio de Justicia, Edición Actualizada a 4 de marzo 2019

¹⁶ MATA MARTÍN Ricardo, *Delincuencia Informática y Derecho Penal*, Edisofer, 2001.

cierto no es un delito propio, se necesitan conocimientos básicos de informática para lograrlo.

Además de lo consagrado en el Código Orgánico Integral Penal, cabe recalcar Leyes internacionales que son de vital ayuda en la legislación nacional, en especial porque estos delitos que se estudian pueden cometerse desde otro país de forma anónima, como se mencionaba, dificultando la investigación penal dentro del país donde se producen los efectos del delito. La Convención Interamericana sobre Asistencia Mutua en Materia Penal tiene como objeto la solución de delitos que se susciten entre países miembros, de la cual el Ecuador es miembro y sin duda al menos a nivel americano, hay mayor respaldo diplomático y judicial para la imputación de delitos. En su artículo 7 del ámbito de aplicación de este tratado, se estipula la cooperación internacional para la recopilación y estudio de las pruebas, traslado de personas detenidas y otras prácticas que pertenecen al debido proceso y garantías en caso de privación de libertad. Con la ayuda de la justicia y autoridades de otros países, de haberse cometido el delito en países de la OEA, facilita la labor investigativa y hay respaldo para esta investigación de delitos¹⁷.

III.a.- Interceptación ilegal de datos (Hacking)

El artículo 230 del COIP que contiene el delito de interceptación ilegal de datos, estipula que la persona que sin consentimiento de una autoridad competente o de la persona natural o jurídica de quien se pretende obtener información, obtenga dicha información mediante medios electrónicos e informáticos, está sujeta a una pena privativa de libertad de tres a cinco años. Los datos informáticos son manejados por administradores informáticos que pueden ser institucionales o personales, su tratamiento se realiza mediante programas de software que facilitan la gestión de dicha información, la interceptación de tales datos se puede realizar mediante el acceso abusivo al sistema que los contiene¹⁸. Para efectos de este trabajo podremos definir aquellas personas que infringen sistemas de seguridad

¹⁷ Convención Interamericana sobre Asistencia Mutua en Materia Penal (Convención de Nassau), Bahamas, 1992.

¹⁸ PABÓN PARRA Pedro Alfonso, *Manual de Derecho Penal Tomo II Parte Especial*, Ediciones Doctrina y Ley Ltda., Bogotá, 2013.

informáticos como *hackers*, que son individuos que exploran los sistemas de información intentando demostrar al máximos sus habilidades, buscando dominar la programación y electrónica, a fin de mejorar sistemas de información complejos, o cometiendo otros delitos¹⁹. La conducta punible es la sustracción de información informática que pueda usada con el fin de causar un perjuicio económico o de información privada que pudiera afectar a la honra de la persona. Sin embargo, lo que representa mayor beneficio económico para el infractor es la información que le permita obtener el patrimonio económico al que aspira y consecuentemente, establecer este delito como medial para la ejecución de los otros que se tratan en este trabajo de investigación académica.

En el análisis objetivo y subjetivo del delito, para el sujeto activo no hay ningún limitante por cuanto puede ser cualquier persona, basta que tenga ciertos conocimientos propios de la informática para poder realizar la conducta prohibida. Del sujeto pasivo, es decir, la víctima del delito, de igual forma puede ser cualquier persona, sea natural o jurídica, del derecho público o privado, instituciones bancarias o crediticias, unidades educativas, gobiernos locales o centrales, todos ellos quienes usan sistemas automatizados de información, generalmente conectados a otros sistemas²⁰.

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema²¹. Particularmente de este delito de interceptación ilegal de datos o de *hacking*, como en la problemática de forma breve se mencionó, este delito a diferencia de otros contra la propiedad como el hurto, robo o apropiación indebida, éste no puede ser objeto de un apropiamiento patrimonial de carácter físico, sino de tener como objeto el acceso a información digital que es atractiva para el infractor, por lo que es un delito medial en la gran mayoría de los casos, a sabiendas que a partir de tener

¹⁹ PÉREZ LUÑO Antonio Enrique, *Manual de Informática y Derecho*, Ediciones Ariel, Madrid, 2006.

²⁰ BLOSSIERS MAZZINI, J.J & CALRDEÓN GARCÍA S., *Los Delitos Informáticos*, Editorial RAO, Lima, 2005.

²¹ ACURIO DEL PINO Santiago, *Delitos Informáticos*, Editorial PUCE, Quito, 2012.

disponibilidad de información financiera para poder vulnerar el patrimonio económico de la víctima, sin excluir la posibilidad de más delitos que se puedan realizar, como la extorsión.

Los cajeros automáticos, tanto su *software* como el *hardware*, son susceptibles de la intromisión ilegal en los sistemas de la información, que consiste en todo acto intencionado y sin autorización para obstaculizar o interrumpir, de manera significativa el funcionamiento de un sistema de la información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos²². Por ello es necesario que constantemente los encargados del sistema informático de los bancos e instituciones financieras actualicen en temas de seguridad la información que contienen de forma digital, para buscar prevenir el cometimiento de este delito, y a su vez, si se llegan a cometer, tener herramientas a la mano para buscar a los infractores.

III.b.- Producción, tenencia y tráfico de instrumentos destinados a la falsificación de moneda

La falsificación de monedas y la falsificación de billetes pertenecen al mismo ámbito fáctico regulativo. El cual, en consecuencia, debería encontrarse descrito más bien en un mismo tipo modelo. El mencionado criterio de sistematicidad se ve también amagado por la regulación nuevamente en otra ley de las hipótesis de falsificación de tarjetas de crédito o débito y de uso de tarjetas falsificadas²³. La relación con este postulado y el delito de producción, tenencia y tráfico de instrumentos para falsificar dinero, es que el delito de estudio es vital para falsificar dinero, porque materialmente resulta imposible falsificar dinero o en el caso de estudio, tarjetas de crédito para poder ser usadas en cajeros automáticos. El artículo 305 del COIP trata producción, tenencia y tráfico de instrumentos destinados a la falsificación de moneda; la conducta típica de este delito radica en los verbos rectores produzca, conserve, adquiera o comercialice.

²² GIMÉNEZ SOLANO Vicente Miguel, *Hacking y Cibercriminología*, Universitat Politècnica de Valencia, 2013.

²³ ROJAS Luis Emilio, *Modelos de Regulación de los Delitos de Falsedad y Delitos Patrimoniales*, Universidad Alberto Hurtado, Santiago, 2017.

Basta que el sujeto activo que puede ser cualquier persona, tenga bajo su dominio estos instrumentos, o tenga como propósito de vender o producirlos.

Consiguientemente, la falsificación de documentos privados tendría una naturaleza ambivalente, revistiendo un carácter análogo al de una defraudación²⁴. El tipo penal va dirigido tanto al que produce así como al que comercializa los insumos que estén destinados a la elaboración de billete moneda, cheques, títulos valores como bonos o acciones al portador, utilizarla como moneda de curso legal en nuestro país. Dada la naturaleza del delito, este del 305 y 306 pertenecen al grupo de delitos contra el sistema monetario del COIP. El tipo penal posee verbos rectores que guían la acción punible, que son de fabricar, introducir y conservar.

Para obtener rédito económico entonces, el sujeto activo, sea de forma directa o por intermedio de facilitadores del delito necesita vender dicha producción de instrumentos dedicados a la falsificación de moneda y tarjetas de crédito o en su defecto, usarlos para poder forjar dinero por su cuenta. Tanto el sujeto activo como pasivo del delito, pueden ser cualquier persona, y el bien jurídico del cual el delito goza tanto en la doctrina como en Ecuador, es el régimen u ordenamiento monetario, es decir, la vigencia plena que tiene el dinero en la sociedad, vigencia que debe gozar además de confianza y credibilidad de la población en el sistema monetario e instituciones financieras. La política criminal está basada entonces, en sancionar desde un inicio meros actos preparatorios antes de que ingresen al tráfico monetario, de manera que estamos ante un delito de peligro abstracto²⁵. Como se aprecia en el desarrollo de estos delitos, vemos una estructuración concatenada tal que muestra que son delitos mediales entre sí para llegar a consumir la estafa, que es finalmente donde quien delinque podrá disponer del patrimonio ajeno.

Este delito se consuma cuando los elementos de producción de moneda falsa se encuentran listos para ser puestos en circulación, sin que precise la

²⁴ MAYER LUX Laura, *La Falsificación de Instrumentos Privados*, Revista de Derecho Universidad Austral de Chile, Valdivia, 2014.

²⁵ REÁTEGUI SÁNCHEZ, *Tratado de Derecho Penal Parte Especial*, Legales Ediciones, Buenos Aires, 2016.

efectividad de los mismos ni el perjuicio a un tercero, o según el COIP también, que se conserven estos materiales que faciliten la fabricación de moneda falsa.

III.c- Falsificación de moneda y otros documentos

La falsificación puede afectar la demanda de moneda si hay pérdida de confianza en el uso de dinero. Por ejemplo, la falsificación puede afectar la función del dinero como reserva de valor y medio de cambio. Es la percepción del riesgo lo que afecta la confianza. La confianza se debilita si el público percibe que hay un riesgo mayor de que podrían estar aceptando dinero falso como pago sin saberlo²⁶. Remitiéndonos al artículo 306 sobre la falsificación de moneda y otros documentos, el legislador nacional optó por incluir dos modalidades en las cuales se puede llevar a cabo el delito, teniendo como punto de partida la falsificación, sin embargo la persona que falsifica no siempre es el encargado de la circulación, por esto los delitos que se tratan en este artículo académico son mediales entre sí, teniendo a la estafa como delito fin.

El segundo inciso del artículo es de nuestro interés, por cuanto se refiere a la falsificación de tarjetas de crédito, así como también otros documentos con valor pecuniario, cuya pena recae sobre quienes forjan estos documentos pertenecientes al sistema monetario. Así, no se ha pausado el intento de identificar un bien jurídico propio y suficientemente expresivo como para justificar tal empeño legislativo, sino que, al contrario, en casi todos los supuestos se ha tenido que reconducir la tipicidad de estas conductas a los tipos tradicionales que protegían el patrimonio y la fe pública²⁷. El legislador considera este segundo inciso merecedor de una pena mayor, como se había considerado, además de afectar al sistema financiero, mediante tecnología y conocimientos aplicados a forjar estas tarjetas y documentos falsos

Además del dolo para viciar en el error al sujeto pasivo de este delito, aparece además el ánimo de lucro o el perjuicio a un tercero, para efectos de la

²⁶ VILES Nathan & RUSH Alexandra, *Los Costos Sociales de la Falsificación de Moneda*, CEMLA, Sidney, 2015.

²⁷ GALÁN MUÑOZ Andrés, *El Fraude y la Estafa mediante Sistemas Informáticos*, Tirant lo Blanch, Valencia, 2005.

falsificación de dinero²⁸. La consumación del delito se da entonces por el solo hecho de la ejecución de la conducta de forjar el dinero ilícitamente, indistintamente si ya se ha puesto en circulación o se lo ha tratado de vender por dinero real. En términos del lenguaje natural y descriptivo, se entiende que la falsificación de moneda es la acción de cambiar, mutar, deformar la moneda nacional o extranjera o en crearla, con cierta apariencia de similitud con la auténtica emitida por los Bancos Centrales de cada país. Por ello, en este delito tanto el sujeto activo como pasivo pueden ser cualquier persona. Sin embargo, el infractor posee ciertos conocimientos de informática y del uso de herramientas que permitan forjar tarjetas de crédito para ser usadas en cajeros automáticos, siendo el bien jurídico para el derecho nacional el régimen monetario, aunque también de forma secundaria se afecta el patrimonio y la fe pública.

Existen en los contratos correspondientes con las entidades emisoras de las tarjetas de crédito o débito para la utilización de la misma, la prohibición de obtener dinero de los cajeros automáticos en exceso del cupo de crédito otorgado; para evitar la superación de los límites de los créditos se programan los cajeros, que en la mayoría de los casos no entreguen más dinero del cupo previsto²⁹. Esta medida sin duda es de gran utilidad para buscar la prevención del delito, puesto que si el usuario se excede del cupo asignado o está llegando al límite de su cupo, es susceptible de recibir dinero falso, que es el daño a causar con el delito de falsificación de dinero.

III.d.- La Estafa

Previo al análisis de la norma delito del artículo 186, que tipifica la estafa, cabe recalcar que la estafa es un delito que ataca al patrimonio en su universalidad, consiste en la disposición patrimonial realizada por la víctima por haber sido inducida (o mantenida) a error por parte del agente, quien se ha servido del engaño u otra actitud fraudulenta. Dicho esto, el artículo 186 del COIP recoge elementos básicos de la doctrina internacional para tratar este injusto penal, dado que menciona que la pena privativa de libertad recae a la persona que mediante

²⁸ VIZUETA, 2011, P.140.

²⁹ SUÁREZ SÁNCHEZ Alberto, *Manipulaciones de Tarjetas Magnéticas en el Derecho Penal Colombiano*, Universidad Externado de Colombia, Bogotá, 2015.

engaños se beneficie del patrimonio ajeno o para una tercera persona. No hay duda de que requiere dolo conforme a las reglas generales. En torno a la posibilidad de cometer la conducta típica con dolo eventual, nos estimamos en contra de ello, dada la naturaleza misma de los elementos del delito. Como se analizará a continuación, el engaño, requisito típico, necesita de una acción concreta y manifestada, aunque sea una simple mentira, siendo difícil imaginar un despliegue fáctico que no esté presidido por un propósito definido³⁰.

En lo que respecta a la estafa, se trata de un delito por el cual una persona mediante fraude, induce a otra a disponer de un bien de su propiedad o de propiedad de un tercero³¹. El problema radica en el caso concreto de la estafa mediante cajeros automáticos, que no es fácil determinar con exactitud al infractor o los infractores, dado a los mecanismos tecnológicos o de *software* que se pudieran cometer, además no es común que el sujeto activo cometa directamente la infracción en calidad de autor.

La estafa es un delito de autolesión, en tanto es la propia víctima quien entrega el bien o termina lesionando o perjudicando su patrimonio, influenciada por el error al que ha sido inducida por el agente del delito³². En la doctrina, los autores concuerdan en que la estafa, la entrega del patrimonio se la hace por parte de la víctima. Sin embargo, la entrega consentida se caracteriza por estar viciada por el error, por el engaño que hace alusión en la doctrina como en la legislación nacional. El error como elemento subjetivo del delito, es un vicio de la conciencia, entendida esta como el grado más alto del conocimiento; quien incurre en este vicio tiene nociones e ideas deformadas sobre un tema, de modo que una es la realidad y otra su apreciación³³. La doctrina en cuanto al delito de estafa, conviene en mantener que el error al cual se induce debe procurar permanecer en la víctima hasta el momento en el que de forma viciada dispone de su patrimonio, lo cual también pasa en las estafas mediante cajeros automáticos o al momento de realizar

³⁰ LEYTON JIMÉNEZ José Francisco, *Los Elementos Típicos del Delito de Estafa en la Doctrina y Jurisprudencia Contemporáneas*, Ministerio Público de Chile, Santiago, 2014.

³¹ BAQUERIZO Jorge Zavala, *Delitos contra la Propiedad*, Editorial Edino, Guayaquil.

³² OTTO, *Delito de Estafa*, Editorial Hammurabi, Buenos Aires.

³³ PÉREZ Luis Carlos, *Derecho Penal Partes General y Especial Tomo V*, Editorial Temis, Bogotá, 2014.

compras con tarjetas de crédito, debido a que es muy posible y de hecho ese es el objetivo de esta modalidad de estafa, haber estudiado las potenciales debilidades por las cuales se pudiere engañar a la víctima y que ésta acceda a disponer de su peculio.

Las posibilidades de fraude del que se pretende un beneficio económico y se determina un perjuicio patrimonial, han encontrado un magnífico marco de expansión en internet y mediante sistemas informáticos, dado a la vulnerabilidad de muchos equipos del usuario, desprovistos de medidas de protección más elementales³⁴. Por esta razón, en el caso concreto de las estafas a través de cajeros automáticos y tarjetas de crédito, es preciso indicar que existe conocimientos de informática, para poder adulterar los cajeros automáticos mediante el uso de herramientas externas o alteraciones del software, además que para forjar tarjetas de crédito es preciso contar con la información crediticia de la víctima y la calidad de los materiales a usar, sumado a la mano de obra que debe ser idéntica al que poseen los bancos y establecimientos de tarjetas de crédito.

³⁴ FERNÁNDEZ TERUELO Javier Gustavo, *Ciberdelitos: Los Delitos cometidos a través de Internet*, Constitutio Criminalis Carolina, Oviedo, 2007.

Conclusión

Para culminar este trabajo de investigación del impacto de los delitos informáticos a través de los cajeros automáticos, se ha dado por sentado que los delitos estudiados tienen una característica secuencial, es decir, que la interceptación ilegal de datos (hacking), junto a la producción y tenencia de instrumentos destinados a la falsificación de moneda y la falsificación de moneda son cometidos en ese orden para culminar en la estafa, en especial si nos remitimos a los numerales 1 y 2 del artículo 186, porque el COIP incluye de forma expresa estas nuevas modalidades por intermedio de tarjetas de crédito y alterando la estructura de los cajeros automáticos. Si bien es cierto son delitos en los que el sujeto activo y pasivo pueden ser cualquier persona, excluyendo la característica de delitos propios, es necesario que quien cometa estos delitos posea ciertos conocimientos de informática y de herramientas tecnológicas, que le permitan tomar ventaja de las estructuras de cajeros automáticos y así vulnerar el patrimonio ajeno.

Además, lo analizado de los delitos también puede servir para que las autoridades de justicia e instituciones financieras, tengan la necesidad permanente de estar a la vanguardia en temas de seguridad informática, en especial con los datos informáticos de los usuarios de tarjetas de crédito o débito, y quienes estén encargados del correcto funcionamiento de los cajeros automáticos. Incluso al tener un mayor seguimiento de la seguridad de las tarjetas de crédito y de los cajeros, se fomenta también que el usuario de los cajeros automáticos esté alerta a

cualquier anomalía que pudiera existir, de esta forma los bancos pueden tomar correctivos inmediatos y precautelar la seguridad tanto de sus clientes, como de los propios bancos.

Bibliografía

ACURIO DEL PINO Santiago, *Delitos Informáticos*, Editorial PUCE, Quito, 2012, pág. 12.

BAQUERIZO Jorge Zavala, *Delitos contra la Propiedad*, Editorial Edino, Guayaquil, 1992, pág. 89.

BLOSSIERS MAZZINI, J.J & CALRDEÓN GARCÍA S., *Los Delitos Informáticos*, Editorial RAO, Lima, 2005, pág. 70.

CÓDIGO PENAL COLOMBIANO (Ley 599 del 2000 actualizada), Bogotá, 2000.

CÓDIGO PENAL DE CHILE, Ministerio de Justicia, Santiago, última actualización. 2011.

CÓDIGO PENAL DE LA REPÚBLICA DEL PERÚ, Ministerio de Justicia, versión actualizada al 16 de octubre 2018, Lima.

CÓDIGO PENAL ESPAÑOL & LEGISLACIÓN COMPLEMENTARIA, Ministerio de Justicia, Edición Actualizada a 4 de marzo 2019.

CONVENCIÓN INTERAMERICANA SOBRE ASISTENCIA MUTUA EN MATERIA PENAL (Convención de Nassau), Bahamas, 1992.

COPMAN SPECTOR Sebastián, *El Delito de Estafa y los Nuevos Medos de Pago*, UOC, Barcelona, 2015, pág. 15.

EGRED Joan Paul, Redacción Justicia, Diario El Telégrafo, Quito, 2019.

FERNÁNDEZ TERUELO Javier Gustavo, *Ciberdelitos: Los Delitos cometidos a través de Internet*, Constitutio Criminalis Carolina, Oviedo, 2007, pág. 28.

GALÁN MUÑOZ Andrés, *El Fraude y la Estafa mediante Sistemas Informáticos*, Tirant lo Blanch, Valencia, 2005, pág. 7.

GIMÉNEZ SOLANO Vicente Miguel, *Hacking y Ciberdelito*, Universitat Politècnica de Valencia, 2013, pág. 40.

GÓMEZ VIEITES Álvaro, *Enciclopedia de la Seguridad Informática 2da Edición*, Editorial Alfaomega, Ciudad de México, pág. 173.

GONZÁLEZ CHUSCA & VIVES ANTÓN, *La Estafa Informática*, Editorial Ibáñez, Madrid, 2006, pág. 60.

JAÉN VALLEJO Juan, *Cuestiones Actuales del Derecho Penal Económico*, Editorial Ad-Hoc, Madrid, 2004, pág. 93.

JAVATO MARTÍN Antonio, *Las Tarjetas de Crédito y Débito (aspectos penales)*, Universidad de Salamanca, 2013, pág. 13.

LEYTON JIMÉNEZ José Francisco, *Los Elementos Típicos del Delito de Estafa en la Doctrina y Jurisprudencia Contemporáneas*, Ministerio Público de Chile, Santiago, 2014, pág. 70.

MARIÑO LÓPEZ Andrés, *Uso Fraudulento de Tarjetas de Crédito por Terceros no Autorizados*, Editorial Marcial Pons, Madrid, 2006, pág. 22.

MATA MARTÍN Ricardo, *Delincuencia Informática y Derecho Penal*, Edisofer, 2001, pág. 14.

MAYER LUX Laura, *La Falsificación de Instrumentos Privados*, Revista de Derecho Universidad Austral de Chile, Valdivia, 2014, pág. 30.

OTTO, *Delito de Estafa*, Editorial Hammurabi, Buenos Aires, 2006, pág. 119.

PABÓN PARRA Pedro Alfonso, *Manual de Derecho Penal Tomo II Parte Especial*, Ediciones Doctrina y Ley Ltda., Bogotá, 2013, pág. 34.

PÉREZ Luis Carlos, *Derecho Penal Partes General y Especial Tomo V*, Editorial Temis, Bogotá, 2014, pág. 236.

PÉREZ LUÑO Antonio Enrique, *Manual de Informática y Derecho*, Ediciones Ariel, Madrid, 2006, pág. 91.

RAMÓN RUIZ Luis, *Uso Ilícito y Falsificación de Tarjetas Bancarias*, Revista de Internet, Derecho y Política UOC, Barcelona, 2013, pág. 16.

REÁTEGUI SÁNCHEZ, *Tratado de Derecho Penal Parte Especial*, Legales Ediciones, Buenos Aires, 2016, pág. 142.

REYNA ALFARO Luis Miguel, *Los Delitos Informáticos*, Justita Editores, Madrid, 2002, pág. 133.

ROJAS Luis Emilio, *Modelos de Regulación de los Delitos de Falsedad y Delitos Patrimoniales*, Universidad Alberto Hurtado, Santiago, 2017, pág. 6.

SUÁREZ SÁNCHEZ Alberto, *Manipulaciones de Tarjetas Magnéticas en el Derecho Penal Colombiano*, Universidad Externado de Colombia, Bogotá, 2015, pág. 22.

VILES Nathan & RUSH Alexandra, *Los Costos Sociales de la Falsificación de Moneda*, CEMLA, Sidney, 2015, pág. 28.

VIZUETA RONQUILLO Juan, *Delitos Informáticos en el Ecuador*, Editorial Edino, Guayaquil, 2011, P.