RESPONSABILIDAD BANCARIA FRENTE AL DELITO DE *PHISHING* EN COLOMBIA

Alexander Zabala

RESUMEN

Considerando la globalización y el avance de las tecnologías de la información y la comunicación (TIC) y su incidencia en la industria financiera, se analiza la responsabilidad del banco frente al delito de suplantación de sitios web para capturar datos personales en Colombia, conocido como *phishing,* en virtud de los riesgos y las amenazas permanentes a las cuales se ve enfrentado el usuario de la banca móvil, las transacciones en Internet, los cajeros electrónicos mediante tarjeta electrónica. Se analiza la controversia de hasta dónde las entidades financieras tienen responsabilidad objetiva frente a sus clientes, cuando se comete un delito por un tercero, es decir, por la ciberdelincuencia, una aproximación desde la perspectiva del derecho y la legislación vigente.

PALABRAS CLAVE: Ciberdelito, responsabilidad bancaria, derechos del consumidor, responsabilidad objetiva

ABSTRACT

Considering globalization and the advancement of information and communication technologies (ICT) and their impact on the financial industry, the bank's responsibility for phishing in websites to capture personal data in Colombia, known as phishing, By virtue of the risks and permanent threats faced by the user of mobile banking, Internet transactions, electronic teller machines by electronic card. It discusses the controversy about the extent to which financial institutions have an objective responsibility towards their clients, when a crime is committed by a third party, that is, by cybercrime, an approximation from the perspective of the law and current legislation.

KEYWORDS: Cybercrime, bank liability, consumer protection, responsibility objective

SUMARIO

CONTENIDO

PÁG.

INTRODUCCIÓN

El fenómeno de la globalización en todos los ámbitos sociales, junto con el avance de las tecnologías de la información y la comunicación, han creado el llamado ciberespacio como un proceso de masificación de acceso a la tecnología, la información y la comunicación, generando grandes amenazas y riesgos para la sociedad, debido a los diferentes ciberdelitos cometidos por la delincuencia que atentan contra la seguridad de naciones, empresas e individuos, lo cual ha conllevado a los gobiernos, las instituciones y organismos internacionales, a plantear la necesidad de hacer un frente común generar barreras tecnológicas, jurídicas y sociales contra los delitos informáticos.

Uno de los sectores que más se ha visto atacado por los delitos informáticos es el de la industria financiera, y con ello la afectación de muchos clientes que han sido presa de la ciberdelincuencia. Con el avance de la tecnología y su incorporación a la banca digital o en línea a través de los *smartphone*, proliferan con mayor intensidad los ataques a las instituciones financieras y a los usuarios a través del llamado *phishing* o suplantación de identidad, término que hace relación al abuso informático caracterizado por intentar adquirir información confidencial de forma fraudulenta. El cibercriminal, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, o incluso utilizando también llamadas telefónicas (Flores Salgado, 2014:23).

El sistema financiero y bancario además de incorporar verdaderos sistemas de protección para evitar riesgos que amenacen la seguridad de la actividad financiera, también les compete generar procesos de educación e información expedita para los usuarios o clientes, que permitan evitar el *phishing* que comprometan las transacciones bancarias físicas o en línea, prevenir los ataques a través de software malicioso y ante todo, garantizar la seguridad de las claves y dispositivos electrónicos, mediante los cuales se realiza transacciones financieras. Frente a la proliferación del ciberdelito en la industria bancaria, especialmente las transacciones a través de la banca móvil, transacciones en línea a través de internet

o cajeros automáticos, cabe plantear la pregunta problema: ¿Cuál es la responsabilidad bancaria frente al delito de *phishing* en Colombia?

Dar respuesta a esta pregunta, encierra gran controversia por cuanto existen dos posturas contrapuestas, la del cliente y la del banco. La posición del cliente o usuario se puede fundamentar en la existencia de una responsabilidad objetiva por parte de los bancos, pues el servicio que se presta es considerado riesgoso y además no se han tomado las medidas de seguridad necesarias, por lo tanto, deben responder por los daños que con esta actividad se puedan producir. En tanto que, la postura del sistema bancario es que no debe aplicar la responsabilidad por riesgo cuando el hecho dañoso ha sido creado por un tercero y por lo tanto no puede achacarse la responsabilidad al banco, además, se alega la existencia de una relación contractual entre las partes y que las disposiciones que se aceptaron por los clientes son vinculantes.

"Se ha dicho que el banco no puede controlar las actuaciones negligentes de la víctima en tanto exista un mal manejo de su información, fue imprudente cuando accedió a las páginas electrónicas del Banco, brindó contraseñas y datos confidenciales a terceros y demás posibilidades" (Rodriguez Zárate, 2014:3). En este contexto, se justifica llevar a cabo un análisis que permita un acercamiento a la comprensión e identificación de posibles vacíos jurídicos que permitan establecer un balance equitativo en la relación banco-cliente, cuando este último es víctima de un delito informático, y de qué manera el banco debe responder a la luz de la legislación vigente.

METODOLOGÍA

La metodología, entendida como el procedimiento empleado para el logro de un objetivo, se desarrolló en la investigación del presente trabajo, ejecutando una clasificación axial de la información obtenida, para después proceder a darle una estructuración lógica, con el fin de poder establecer un orden de tal manera que fuera posible analizar el contenido, dando como resultado las conclusiones sobre el

tema propuesto

1. ANÁLISIS DE TIPO PENAL, ARTÍCULO 269G CÓDIGO PENAL COLOMBIANO

1.1. TIPO PENAL A LA LUZ DEL DERECHO Y LA TECNOLOGÍA

Desde hace muchos años se viene trabajando el concepto de delito informático o delito electrónico, puesto que el avance tecnológico es imparable, así mismo las nuevas formas de delinquir evolucionan y con ellas los problemas de protección de la información de las personas del común y de las organizaciones o empresas a nivel nacional e internacional. De acuerdo a esto, diversos expertos en el campo de la informática y también del derecho penal así como el informático han dado sus puntos de vista sobre el concepto de delito informático así: Según el experto italiano Carlos Sarzana en su obra *Criminalita e tecnología* se define como delito informático a "los crímenes por computadora comprenden cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo" (AADAT, 2017:12).

Por su parte, María de la Luz Lima dice que el delito electrónico "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin" (AADAT, 2017:14). En este sentido, se puede observar que la delincuencia va mucho más allá de la comisión de un delito como tal de forma física, ya que se busca facilitar la materialización de los mismos mediante el uso de los recursos tecnológicos disponibles, es aquí donde la conceptualización del delito informático en forma típica y atípica surge como lo conceptualiza Julio Téllez Valdez entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" (Tellez Valdez, 1996:1).

En el 2001 en la ciudad de Budapest se llevó a cabo el primer congreso contra la cibercriminalidad, en este proceso intervinieron los países asociados a la Organización de la Naciones Unidas (ONU) en donde se promulgó un convenio o tratado que busca identificar, tipificar y establecer un conjunto de normas contra la delincuencia cibernética o delitos informáticos a nivel internacional como modelo a tratarse en cada país, con el fin de mitigar los efectos adversos de este tipo de acciones ilegales en contra de los bienes tanto económicos como morales a los que se ven expuestos las personas actualmente con el uso de la tecnóloga en cada ámbito.

Este convenio agrupa de acuerdo a su definición y enfoque los delitos informáticos de la siguiente manera: Título I: Delitos contra la confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos. (Art. 2) Acceso ilícito, (Art. 3) Interceptación ilícita, (Art. 4) Ataques a la integridad de los datos, (Art. 5) Ataques a la integridad del sistema, (Art. 6) Abuso de los dispositivos. Título II: Delitos informáticos, (Art. 7) Falsificación informática, (Art. 8) Fraude informático. Título III: Delitos relacionados con el contenido, (Art. 9) Delitos informáticos relacionados con la pornografía infantil. Título IV: Delitos relacionados con infracciones de la propiedad intelectual y derechos afines, (Art. 10) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (COE, 2017).

En Colombia dentro del marco legal establecido el 5 de Enero de 2009 mediante la Ley 1273, se realizó un trabajo de tipificación o clasificación de los delitos informáticos en donde de acuerdo a su comisión se clasifican en 9, para efectos de este trabajo, solo tomaremos el numeral 7: Suplantación de sitios web para capturar datos personales. Este delito hace referencia al famoso Phishing y hace parte de los ataques de ingeniería social, los cuales se han perpetuado valiéndose de las vulnerabilidades no de los sistemas informáticos sino de los errores o fallos humanos, mediante los cuales logran conseguir datos personales

que puedan servir para engañar y sustraer información.

Este tipo de actividades delictivas utilizan varias formas de operar como por ejemplo llamadas telefónicas, envió de correos electrónicos en donde solicitan información sensible como claves de tarjetas de crédito o inclusive en forma física con identificaciones falsas para lograr el acceso a sitios no autorizados al público en las entidades.

1.2. ELEMENTOS DEL TIPO

En el Código Penal colombiano, el Artículo 269G se refiere expresamente a la suplantación de sitios web para capturar datos personales, definiéndolo como “el que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave” (Arboleda V & Ruiz S., 2015: 1161). De igual manera, agrega el Código, “en la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que accede a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave” (Arboleda V. & Ruiz S., 2015: 1161)

El Código también define y delimita el ciberdelito conocido como phishing, describiéndolo como “la suplantación de identidad que tiene por finalidad apropiarse de datos confidenciales de los usuarios” (Arboleda V. & Ruiz S., 2015: 1161). Se trata de una forma de spam usados de forma perniciosa, poniendo el peligro la integridad de la información sensible de los usuarios y provocando, incluso, graves consecuencias. El *phishing*, junto a los programas de espías, representa una de las técnicas más empleadas para hurtar información a través de internet. “Para que la conducta se tipifique como punible, necesario es que el agente actúe con un objeto

ilícito; si no hay ilicitud no habrá delito. Paralelamente, no debe estar autorizado o facultado" (Arboleda V. & Ruiz S., 2015: 1161). A continuación, se describen las características del delito, los sujetos, la conducta y la pena.

El abogado de la Universidad Autónoma de México, Julio Téllez Valdez, presenta las siguientes características de un delito informático: i) Conducta criminal de cuello blanco, pues solo alguien o un pequeño grupo de personas con los conocimientos necesarios puede cometerlos; ii) Acciones ocupacionales, pues se realizan a sujetos que están laborando; iii) Acciones oportunistas, pues se aprovechan de una necesidad creada o intensificada dentro del sistema tecnológico y económico; iv) Provoca serias pérdidas económicas, ya que el único beneficiario es el "hechor"; v) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una presencia física necesaria, puede consumarse el hecho; vi) Son muchos los casos y pocas las denuncias, esto debido a la falta de regulación por parte del Derecho; y vii) Presentan grandes dificultades para su comprobación, por su mismo carácter técnico (Manjarrés Bolaño & Jiménez Tarriba, 2012:5).

Sujeto activo: Según Mario Garrido Montt (1992:5) "se entiende por tal, quien realiza toda o una parte de la acción descrita por el tipo penal". De igual forma, Edwin Sutherland, criminólogo norteamericano, ya en el año 1943 había señalado que "el sujeto activo del delito es una persona de cierto *status* socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional".

Generalmente, el sujeto activo, en la genralidad de los delitos informaticos, se trata de personas que poseen un alto conocimiento en el manejo de los sistemas informaticos y en las tecnologías de la comunicación.

Bajo el anterior contexto, se puede decir que el sujeto activo, para el delito

contemplado en el artículo 269G del Código Penal colombiano, es indeterminado, ya que el mismo artículo lo define como: "*el que*", con objeto ilicito y sin estar facultado.

Sujeto pasivo: El sujeto pasivo según Manjarrés & Jiménez (2012:6), "es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo". Previamente, hay que distinguir que el sujeto pasivo es el ente sobre el cual recar la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos, las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etc., que utilizan diferentes y variados sistemas automatizados de información.

El delito de phishing tiene dos elementos pasivos especiales, que exige que el sujeto activo lleve a cabo una serie de acciones, con el fin de suplantar, sin estar facultado para ello y además con objeto ilicito, se puede decir que los sujetos pásivos son el usuario, quien en el proceso termina entregando su información personal y de sus productos financieros, y la entidad bancaria a la cual han suplantado mediante la falsificacion de la página web o el envio de mensaje electronico fraudulento, entre otros, ya que son ellos, usuario y entidad, quienes hacen uso de los sistemas que utilizan las tecnologias de la informacion y las comunicaciones, adulteradas por la ciberdelincuencia.

Conducta: La conducta en el delito de Phishing, consite en lo que indica el verbo rector, dentro del artículo en mensión, el cual, y señalando las actividades de: *"diseñe, desarrolle, trafique, venda, ejecute, programe, o envié páginas electrónicas, enlaces o ventanas emergentes"* (2012:6), establece de esa manera la configuracón del delito, adecuandolo en esas conductas.

Pena: Las penas "se dividen en principales, sustitutivas y accesorias privativas de otros derechos, cuando no obren como principales" (Botero M. Javier & älvarez Sandra, 2011:691), la pena para el tipo penal del artículo 269G del Código penal

colombiano, quedó determinada en prisión de cuarenta y ocho (48) a noventa y seis (96) meses de prisión y en multa de 100 a 1.000 salarios mínimos legales vigentes, con la salvedad, que la conducta no constituya otro delito, que sea sancionado con una pena más grave (2012:6).

2. ANÁLISIS DE RESPONSABILIDAD OBJETIVA BANCARIA FRENTE AL TIPO PENAL DEL ARTÍCULO 269G DEL CÓDIGO PENAL COLOMBIANO

2.1. CONCEPTO DE LA RESPONSABILIDAD OBJETIVA

"La responsabilidad objetiva se basa en la inobservancia de normas de cautela, antes que en una valoración del actuar de la persona y de sus perfiles subjetivos" (Diez-Picazo, 1999:333). Por su parte, la responsabilidad subjetiva se funda exclusivamente en la existencia de culpa por parte de un sujeto, en tanto que la responsabilidad objetiva no exige tal requisito.

Doctrinalmente se ha entendido que "el daño es la razón de ser de la responsabilidad, y por ello, es básica la reflexión de que su determinación en sí, precisando sus distintos aspectos y su cuantía, ha de ocupar el primer lugar, en términos lógicos y cronológicos, en la labor de las partes y del juez en el proceso. Si no hubo daño o no se puede determinar o no se le pudo evaluar, hasta allí habrá de llegarse; todo esfuerzo adicional, relativo a la autoría y a la calificación moral de la conducta del autor resultará necio e inútil. De ahí también el desatino de comenzar la indagación por la culpa de la demandada". En este mismo sentido afirma Henao que "el estudio del daño puede y debe, entonces, aislarse del estudio del conjunto de la responsabilidad. Se trata de hacer la separación entre la responsabilidad y el punto de partida", y más adelante, "el daño es un requisito indispensable para que surja la responsabilidad civil; es más, es su punto de partida".

Según lo anterior, es necesario, entonces, establecer su existencia y su alcance en aras de obtener una efectiva y debida reparación, es decir, la

traslación patrimonial a favor de la víctima y en contra del responsable o responsables, especialmente cuando se manifiesta en intereses o bienes colectivos. Por tal motivo, es racional entender que el daño sea el punto de partida en el estudio de la responsabilidad. Así pues, el daño es un presupuesto fundamental pero no suficiente para la existencia de la responsabilidad, puesto que es necesaria la presencia de otros elementos que completen su estructura. Se puede precisar, entonces, que el daño se debe entender como la alteración, perjuicio, depreciación, aminoración patrimonial, vulneración o menoscabo de una situación favorable que sufre una persona en su integridad o en sus bienes.

2.2. ELEMENTOS DE LA RESPONSABILIDAD OBJETIVA

“La responsabilidad objetiva significa la obligación de responder o de indemnizar que se origina en la relación causa efecto entre el hecho-causa y el hecho-consecuencia y según esta visión, los elementos necesarios para que se configure la responsabilidad objetiva son el obrar humano y el perjuicio, unidos por un nexo causal. En sentido más amplio, la responsabilidad objetiva hace referencia a los sistemas que se oponen al de responsabilidad subjetiva” (Peirano Facio, 2004:6).

Se trata entonces de establecer un régimen de responsabilidad para quienes ejercen una actividad de la cual obtienen provecho a través del riesgo de tal actividad y que de alguna manera ejercen una posición dominante frente a quien recibe el daño, teniendo presente que habrá lugar a exonerarse de tal responsabilidad cuando medie culpa de la víctima, como en el caso del uso de los medios electrónicos de pago donde se demuestre que el cliente o usuario ha sido negligente y la teoría del riesgo creado puede aplicarse en aquellos casos en los que la ley lo contemple. Para un mejor análisis debe tenerse en cuenta que, el daño es el elemento esencial y necesario para que se configure la responsabilidad, por eso resulta racional estudiarlo a partir de la teoría general, porque este existe por sí solo, como concepto objetivo, sin embargo la responsabilidad no puede subsistir sin su presencia.

2.3. JURISPRUDENCIA SOBRE LA RESPONSABILIDAD OBJETIVA

La Corte Suprema de Justicia en Sentencia SC18614-2016 de Diciembre 19 de 2016, resolviendo un recurso de casación, indico que: Las entidades financieras “deben reparar perjuicios ocasionados por fraudes electrónicos, se advierte que las entidades financieras deben asumir la responsabilidad por la defraudación sufrida por sus usuarios a través de transacciones electrónicas y reparar, en consecuencia, los prejuicios sufridos por estos actos, en efecto, se explica que ese riesgo es inherente a la actividad bancaria, la cual se caracteriza por ser profesional, habitual y lucrativa, cuya realización requiere, además, de altos estándares de diligencia, seguridad, control, confiabilidad y profesionalismo. Lo anterior conduce a la innegable e ineludible obligación de garantizar la seguridad de las transacciones que autoriza por cualquiera de los medios ofrecidos al público, con independencia de si los dineros sustraídos, provienen de cuentas de ahorro o de cuentas corrientes, no obstante, se aclara que un banco, puede exonerarse si prueba que el fraude ocurrió por culpa del cuentahabiente o que su actuar dio lugar al retiro de dinero de la cuenta, transferencias u otras operaciones que comprometieron sus recursos, pues si bien es el usuario quien tiene el control de los mecanismos que le permiten hacer seguimiento informático a las operaciones, a través de controles implantados en los software especializados con los que cuentan, se recuerda que la culpa incumbe demostrarla a quien la alegue”.

Con ese fallo, la Corte Suprema de Justicia, determinó que el sistema bancario será responsable con la seguridad de las transacciones de sus clientes, hechas a través de medios electrónicos, aunque la entidad bancaria podrá exonerarse de dicha responsabilidad, siempre y cuando pueda probar que el fraude ocurrió por descuido o culpa del cuentahabiente. Pero en concreto, es el banco quien debe mejorar la pedagogía con sus clientes, con el objetivo de minimizar el riesgo de fraude, a través de la modalidad de *phishing.*

3. ANÁLISIS DE RESPONSABILIDAD SUBJETIVA BANCARIA FRENTE AL TIPO PENAL DEL ARTÍCULO 269G DEL CÓDIGO PENAL COLOMBIANO

3.1. CONCEPTO DE LA RESPONSABILIDAD SUBJETIVA

"El régimen de responsabilidad subjetiva se fundamenta en la noción de culpa, es decir, en la intención de inferir daño por parte de su causante, o el grado de negligencia que genera tal daño. Así, el mecanismo principal para determinar la ausencia de responsabilidad por parte del causante del daño es la demostración de la diligencia que le es exigida en el caso particular" (Rodriguez Zárate, 2014:292).

3.2. ELEMENTOS DE LA RESPONSABILIDAD SUBJETIVA

Ante la ausencia de una legislación o marco jurídico pertinente para el establecimiento de los sujetos responsables en la provisión, distribución y uso del internet, es el Código Civil que en su esencia y fundamentación se puede asimilar a un posible establecimiento de responsabilidad por los delitos y culpas, que según Peña Valenzuela, comprende los artículos 2341° a 2360°, donde se señalan los parámetros principales del esquema general de responsabilidad civil extracontractual en Colombia, que ha sido complementado por la doctrina y la jurisprudencia especialmente en lo pertinente al establecimiento de las teorías clásicas de responsabilidad subjetiva (daño, conducta, nexo causal, culpa) y responsabilidad subjetiva (daño, conducta, nexo causal).

Es en este marco que se puede atribuir responsabilidad civil de las personas jurídicas y responsabilidad de los proveedores de servicio de internet PSI dado que son agentes de riesgo. Pero también puede extralimitarse la postura en tanto que los PSI son meros intermediarios o mandatarios y es en ese sentido que la jurisprudencia internacional en sus fallos los ha catalogado. "En todo caso se debe partir del supuesto de que por tratarse de responsabilidad subjetiva, la entidad bancaria está obligada a desarrollar sus actividades tendientes a brindar seguridad en transacciones electrónicas con el mayor grado de diligencia, pero no puede garantizar un resultado, pues trascendería entonces su obligación al ámbito de la

responsabilidad objetiva” (Rodríguez Zárate, 2014:292).

3.3. JURISPRUDENCIA SOBRE LA RESPONSABILIDAD SUBJETIVA

La Corte Constitucional, con respecto a la culpa, ya lo menciona en la Sentencia C-155/02, “que la jurisprudencia constitucional ha sido reiterativa en exigir la culpabilidad como elemento esencial para derivar responsabilidad, lo que implica que sólo son sancionables las faltas que son cometidas a título de dolo y de culpa en virtud de ello el operador jurídico debe remitirse a las previsiones del Código Penal y de Procedimiento Penal”.

Continua la sentencia explicando que “no resulta suficiente que se establezca la existencia o comisión de la falta y se determine su autor, sino que se debe determinar la culpabilidad (a título de dolo o culpa), para definir el grado de levedad o gravedad de la falta (Art. 27°, numeral 1, Ley 200 de 1995), todo ello soportado en las pruebas debidamente decretadas, practicadas, controvertidas y allegadas, para proteger las garantías constitucionales del derecho de defensa y presunción de inocencia”. Esta sentencia pone de manifiesto que no solo basta con precisar la culpa, sino que ésta debe ser determinada bien a título de dolo o de culpa pero debidamente fundamentada.

De conformidad con el artículo 1604° del Código Civil, la entidad emisora del medio de pago seria quien estaría en la obligación de probar que actuó en forma diligente, por lo que al titular de dicho medio de pago solo le incumbe afirmar que sus perjuicios derivaron del incumplimiento contractual de parte de la entidad financiera. “Teniendo en cuenta que la responsabilidad contractual parte de presumir la culpa, se invierte la carga de la prueba y entonces no corresponde al titular del medio de pago probarla, sino al emisor acreditar su diligencia” (Rodriguez Zárate, 2014:294).

4. RELACIÓN ENTRE EL TIPO PENAL Y LAS RESPONSABILIDADES OBJETIVA Y SUBJETIVA PARA DETERMINAR LA RESPONSABILIDAD BANCARIA EN EL TIPO DEPANL DEL ARTÍCULO 269G

4.1. DE LA RESPONSABILIDAD OBJETIVA

Antes de la firma del TLC con Estados Unidos y como preparación de la entrada en vigencia del Tratado derivado de las discusiones previas, el gobierno presentó ante el Congreso de la República el Proyecto de Ley 241 de 2011, el cual tenía como único propósito determinar la responsabilidad de los intervinientes en las transmisiones digitales y su contenido más cercano al Digital Millenium Copyrigth Act (DMCA) de 1988 de los Estados Unidos, cabe anotar que fracasó el Proyecto de Ley 241 de 2011 más conocido como Ley Lleras, quedando Colombia, en ese momento, en un limbo jurídico sobre el particular con el agravante de dar cumplimento a los TLC que ha firmado con diversos países y que especialmente Estados Unidos ha incorporado expresamente la obligación para el país de regular la responsabilidad de los ISP, sin embargo, se trae a colación este proyecto por cuanto establecía diferentes pautas acerca de responsabilidad por el uso de datos en el ciberespacio.

El proyecto de Ley buscaba definir el alcance de la responsabilidad de los actores que necesariamente intervienen para que se lleve a cabo este tipo de infracción, con el propósito de identificar posibles medidas que en un escenario de oferta y demanda pudieran cumplir una función similar a los planteados por esa ley, bajo parámetros de ciberespacio.

Los responsables. El proyecto de Ley en su artículo 2 establecía que los responsables por el uso de los contenidos son los prestadores de servicio de Internet, los proveedores de contenido, y los usuarios, de conformidad con las normas generales sobre responsabilidad civil, penal y administrativa.

El bien protegido: El mismo artículo 2 establecía que es la información utilizada

en sistemas o redes de información debe ser objeto de protección por la legislación sobre derecho de autor y derechos conexos.

Limitación a la responsabilidad: los prestadores de servicios de Internet no tendrían la obligación de supervisar los datos que transmitan, almacenen o refieran, ni de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas. Sin embargo, que la autoridad competente podía ordenar a los ISP realizar actividades para investigar, detectar y perseguir este tipo de delitos o infracciones.

Exoneración de responsabilidad: los prestadores de los servicios señalados por la ley no serían obligados a indemnizar el daño que se cause a terceros a través de sistemas o redes controlados u operados por ellos siempre que cumplan con las condiciones previstas en la ley.

La responsabilidad por la transmisión de datos, el enrutamiento y el suministro de conexiones: los prestadores de estos servicios no serían responsables de los datos transmitidos siempre que no modificaran ni seleccionaran el contenido, no iniciaran la transmisión, no seleccionaran a los destinatarios, o establecieran condiciones para la finalización de los contratos de los proveedores de contenido que sean infractores, no interfirieran en las medidas tecnológicas de protección y gestión de derechos de obras protegidas, y no generaran ni seleccionaran el material o a sus destinatarios.

Atribuciones del juez: podría disponer la aplicación de medidas para bloquear el acceso a determinado contenido infractor o supuestamente infractor.

Almacenamiento temporal de datos mediante procesos automáticos: el proyecto de Ley en su artículo 6 establecía las condiciones que deben cumplir los prestadores de este servicio para que no sean responsables de los datos que almacenan; dentro de las condiciones se menciona la de no tener conocimiento

efectivo del supuesto carácter ilícito de los datos, no recibir beneficio económico en los casos en que tenga el derecho y la capacidad de controlar la actividad, y designe a un responsable de recibir las notificaciones judiciales y un medio para recibir solicitudes de retiro o inhabilitación de material. De igual manera el artículo 7 hace lo propio respecto de los prestadores de servicios de almacenamiento a petición del usuario en sistemas o redes controlados u operados por o para dichos prestadores. Las atribuciones de los jueces ante infracciones relacionadas con este tipo de servicio eran limitadas por la ley al retiro o inhabilitación del acceso al material correspondiente.

Servicio de referir o vincular sitios web mediante herramientas de búsqueda: las obligaciones que deben cumplir las personas que cumplen este tipo de servicios incluyen el desconocimiento del supuesto carácter ilícito de los datos, no recibir beneficio económico atribuible a la actividad infractora, y designar a un responsable de recibir las notificaciones judiciales y un medio para recibir solicitudes de retiro o inhabilitación de material.

Como se describió, cada una de las personas que prestan los diferentes tipos de servicios relacionados con ciberinformación que pueda estar protegida, solo serían responsables ante la ley por su participación en infracciones en la medida en que excedan las funciones propias del servicio que cada uno presta; también son considerados responsable en aquellos casos en que reciban algún beneficio económico atribuible a la comisión de esas infracciones. Así mismo estas personas deben designar a un representante que tramite las quejas y solicitudes relacionadas con estas prácticas, ya sea que provengan de los presuntos afectados por las mismas o de las autoridades encargadas de establecer medidas preventivas o correctivas frente a las mismas.

En cuanto a la responsabilidad que le corresponde a los bancos por la utilización de canales de distribución de servicios financieros, por la intervención de terceros se puede aplicar el régimen de responsabilidad presunta consagrado en la Ley 1480

de 2011, el cual está establecido en el artículo 78 de la Constitución Política de Colombia de 1991, en cuanto que los bancos prestan servicios financieros y no se excluyen de la normativa general contenida en el Estatuto de Protección del Consumidor.

Si la actividad causante del daño se origina en la intervención de un tercero, como un hacker, y la entidad bancaria atribuye el resultado a ese hecho para eximirse de responsabilidad, debe analizarse que estamos frente a una actividad de consumo y en consecuencia puede aplicar la protección contenida en la Ley 1480 de 2011 y se puede dejar de lado la relación contractual que refleja una posición dominante del banco frente al cliente, y debe atenderse al criterio del interés público y al riesgo que envuelve el uso del medio electrónico para determinar a quién se le atribuye el daño pero esto no significa que haya mala fe en el actuar del sistema bancario.

La misión del Estado en su intención de construir un marco jurídico legal en la sociedad del conocimiento, de la información y la comunicación consiste entonces en identificar los principales sujetos que intervienen en la Internet según su ámbito de actuación y labor que realice enmarcados como los ISP como parte de un operador de telecomunicaciones (sujeto identificable por su infraestructura tecnológica y su infraestructura física), el proveedor de contenido y el usuario que puede actuar en las redes desde dos roles: como agente y como usuario que puede transformarse en otro rol de generador o publicador de contenido en la Internet.

El concepto del riesgo permite elaborar una teoría que sugiere analizar la posición contractual de las partes, su grado de conocimiento y experiencia en la actividad, lo cual hace posible atribuir a los bancos el deber de reparar el daño producto de uso de medios transaccionales de pago, aunque no medie culpa de parte del cliente o del banco. Cabe indicar que el hecho de que el régimen de responsabilidad sea objetivo no implica que no existan causales que eximan de

responsabilidad a la entidad emisora del medio electrónico de pago.

4.2. DE LA RESPONSABILIDAD SUBJETIVA

Ante la ausencia de una legislación o marco jurídico pertinente para el establecimiento de los sujetos responsables en la provisión, distribución y uso del Internet, es el código civil que en su esencia y fundamentación se puede asimilar a un posible establecimiento de “responsabilidad por los delitos y culpas”, que comprende los artículos 2341 a 2360, donde se señalan los parámetros principales del esquema general de responsabilidad civil extracontractual en Colombia, que ha sido complementado por la doctrina y la jurisprudencia especialmente en lo pertinente al establecimiento de las teorías clásicas de responsabilidad subjetiva (daño, conducta, nexo causal, culpa) y responsabilidad subjetiva (daño, conducta, nexo causal). Es en este marco que se puede atribuir responsabilidad civil de las personas jurídicas y responsabilidad de los proveedores de servicio de Internet PSI dado que son agentes de riesgo. Pero también puede extralimitarse la postura en tanto que los PSI son meros intermediarios o mandatarios y es en ese sentido que la jurisprudencia internacional en sus fallos los ha catalogado.

En todo caso se debe partir del supuesto que, por tratarse de responsabilidad subjetiva, la entidad bancaria está obligada a desarrollar sus actividades tendientes a brindar seguridad en transacciones electrónicas con el mayor grado de diligencia, pero no puede garantizar un resultado, pues trascendería entonces su obligación al ámbito de la responsabilidad objetiva

CONCLUSIONES

Para finalizar, del desarrollo analítico y argumentativo sobre el sistema bancario y la responsabilidad frente al fraude informático en Colombia, se pueden derivar las siguientes conclusiones:

- Que lo analizado, hasta este punto, permite reforzar la idea de que si el banco colocó un portal virtual u otro medio electrónico, se beneficia porque su actividad de captación y colocación exige que exista dicho instrumento para que los clientes puedan hacer efectivo el producto tomado de tal forma que si tal instrumento es permeado por personas ajenas a la relación contractual, y genera pérdidas y daños para el cliente, el que estaría llamado a la reparación es el banco porque su posición contractual es privilegiada y, porque colocó el riesgo luego debe asumirlo, y no se puede pretender que el cliente asuma la pérdida cuando el servicio ofrecido y aceptado por el cliente se hizo en esquemas de seguridad y confianza. Una conducta así desconocería el principio de la buena fe.

- Que la confianza en los bancos es el eje central para que funcione la relación entre estos y sus clientes, de hecho, la actividad financiera es catalogada en la Constitución Política, como una actividad de interés público, ejercida por profesionales calificados, y no como un servicio público, esto les exige a las entidades bancarias un nivel de cuidado y precaución muy alto. Lo cual se traduce en una adecuada protección de clientes y consumidores financieros, con el objetivo de consolidar la confianza en el mercado.

- Que, si bien es cierto, que es obligación del banco reparar el daño ocasionado por un tercero, es posible eximir su responsabilidad, siempre y cuando alegue y demuestre que la culpa, reside en el cliente, por su negligencia en el manejo de sus productos financieros, a través de los canales transaccionales electrónicos y virtuales.

- Que la globalización y la irrupción de las tecnologías de la información y la comunicación, han generado cambios muy significativos en las relaciones de países, organizaciones, empresas y ciudadanos, permitiendo intercambios de todo tipo, generado también, permanentes amenazas en términos de riesgos informáticos, hasta convertirse en verdaderos flagelos para las empresas, especialmente la industria financiera, con los consecuentes impactos en los clientes por el cibercrimen.

- Que se ha generado una permanente controversia entre el sector financiero y bancario frente a su responsabilidad objetiva con sus clientes, por cuanto las dos partes se ven amenazadas por un tercero, el ciberdelincuente, que afecta la relación contractual, presentándose una problemática compleja para el derecho y la legislación en esta materia, por cuanto el Estado debe dar una respuesta justa y equitativa a las partes involucradas, sin embargo, los vacíos jurídicos son latentes por cuanto el ciberdelito rebasa las fronteras y el concepto de Estado-Nación.

- Que la tendencia de los países a su inserción en el mercado mundial a través de diferentes tratados y acuerdos comerciales, implica también involucrarse en la necesidad de establecer convenios y frentes comunes para enfrentar el *phishing*, como modalidad delictiva latente, lo cual enfrenta la necesidad de incorporar reformas legales en el derecho interno o *hard law*, teniendo como marco el derecho blando o *soft law* proveniente de estancias internacionales y de acuerdos o convenios multilaterales.

- Que a la luz del derecho y la legislación vigente en Colombia, no hay claridad con respecto a la responsabilidad contractual del sistema financiero frente al cliente, sin embargo, se han hechos avances significativos en materia de protección al consumidor, que en el contexto derecho comparado, muchos países han implementado, como sinónimo de competitividad e integración a la economía

globalizada, reclamando con justicia mayor protección para el cliente o consumidor frente a los abusos de la parte en posición dominante.

- Que los resultados de este análisis sobre la responsabilidad del sistema bancario frente al *phishing* en Colombia, indican que el problema representa un permanente desafío para el Estado, la comunidad internacional y los organismos especializados, así como la comunidad académica, en sentar jurisprudencia y actualización normativa para poder hacer frente a la problemática de la ciberdelincuencia que con sus ataques, genera graves perjuicios al sector empresarial y a usuarios y consumidor.

- Que frente a la vulnerabilidad y violación que representa la irrupción del internet en todos los aspectos económicos, políticos, culturales, sociales y jurídicos de la sociedad, de un país en particular, y la sociedad global en general. Si bien Colombia se ha preocupado por legislar normas, existen algunos vacíos que requieren de mayor voluntad política y reformas del marco jurídico acorde a la comunidad internacional, especialmente teniendo en cuenta el convenio de Budapest y en general los tratados y acuerdos bilaterales y multilaterales donde el combate al ciberdelito también es cuestión de alianzas y colaboración entre países.

- Que también se hace necesario legislar sobre la responsabilidad de las instituciones financieras, en tanto que deben garantizar la protección del patrimonio de los usuarios y por lo tanto, les compete ser más responsables frente a hechos delictivos acometidos por la ciberdelincuencia. No basta con legislar discursivamente, hace falta crear, dotar y acompañar a las entidades necesarias para el cabal cumplimiento de lo que fue promulgado en la ley, ofreciendo, verdaderamente posibilidades al consumidor-usuario.

BIBLIOGRAFÍA

- AADAT. (20 de Agosto de 2017). Asociación argentina de derecho de alta tecnología. Obtenido de http://www.aadat.org/delitos_informaticos20.htm
- Agencia EFE. (15 de Octubre de 2015). Agencia EFE. Obtenido de http://www.efe.com/efe/america/economia/el-98-5-por-ciento-de-los-riesgos-bancarios-en-america-latina-son-informaticos/20000011-2738875
- Arboleda Vallejo, M., & Ruiz Salazar, J. A. (2015). Código Penal comentado. Bogotá D.C.: Leyer.
- Asociación argentina de derecho de alta tecnología. (20 de Agosto de 2017). AADAT. Obtenido de http://www.aadat.org/delitos_informaticos20.htm
- COE. (20 de Agosto de 2017). Council of Europe. Obtenido de http://www.coe.int/es/web/conventions/home
- Criminológicas, I. d. (2015). Derecho Penal y Criminología, 17-50.
- Diez-Picazo, L. (1999). Derecho de Daños. Madrid: S.L. CIVITAS EDICIONES.
- Flores Salgado, L. (2014). Derecho Informático. México D.F.: Patria.
- Garrido Montt, M. (1992). Nociones fundamentales de la teoría del delito. Santiago de Chile: Editorial Jurídica de Chile.
- Liberos, E., García del Poyo, R., Gil Rabadán, J., Merino, J., & Somalo, I. (2011). El Libro del Comercio Electrónico. Madrid: ESIC.
- Manjarrés Bolaño, I., & Jiménez Tarriba, F. (2012). Caracterización de los delitos informáticos en Colombia. Pensamiento Americano, 71-82.
- Negas, M., Lopes, J., & Do Rosario Negas, E. (2013). Homebanking users and more relevant security risks associated. Iberian Conference on Information Systems and Technologies, CISTI 2013. Lisboa: University of Lisbon.
- Ossorio, M. (1979). Diccionario de Ciencias Jurídicas, Políticas y Sociales. Buenos Aires: Heliasta.
- Peirano Facio, J. (2004). Responsabilidad Extracontractual 2° Edición. Bogotá: Temis.
- PORTAFOLIO. (30 de Octubre de 2015). Portafolio.co. Obtenido de http://www.portafolio.co/economia/finanzas/denuncias-ciberdelitos-crecen-25-

colombia-26308

- Rodriguez Zárate, A. (2014). Análisis económico de la responsabilidad bancária frente a los fraudes electrónicos: El riesgo provecho, el riesgo creado y el riesgo profesional. Bogotá D.C.: Javeriana.
- Tellez Valdez, J. (1996). Los delitos informáticos. Situación en México. Informática y Derecho No. 9, 10, 11.
- UIT. (2003). Declaración de Principios "Construir la Sociedad de la Información: Un desafío global para el nuevo milenio". Cumbre Mundial sobre la Sociedad de la Información. Ginebra: ONU.
- Villalba Cuellar, J. (2012). Análisis de la Ley 148 de 2011, que reforma el Estatuto de Protección al Consumidor en Colombia. Principia Iuris, 32-63.
- Araque Moreno Diego (2011). Derecho Penal Parte General - Fundamentos 2° Edición. Medellín: Universidad de Medellín.