Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas
Año VII. Vol. VII. N° 2. Edición Especial. 2022-II
Hecho el depósito de Ley: FA2016000064
ISSN: 2542-3371
FUNDACIÓN KOINONIA (F.K). Santa Ana de Coro, Venezuela

http://dx.doi.org/10.35381/racji.v7i2.2366

Análisis jurídico de la responsabilidad bancaria frente a delitos informáticos

Legal analysis of banking liability for cybercrime

Ingrid Joselyne Díaz Basurto
ug.ingriddiaz@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Quevedo, Los Ríos
Ecuador
https://orcid.org/0000-0003-2934-4010

Mishelle Katherine Bodero Solis
dp.mishellekbs@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Quevedo, Los Ríos
Ecuador
https://orcid.org/0000-0003-2111-1458

Lenin Gabriel Ulloa García
da.leningug52@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Quevedo, Los Ríos
Ecuador
https://orcid.org/ 0000-0002-8864-3072

Dina Lisseth Mora Nupia
dq.dinalmn26@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Quevedo, Los Ríos
Ecuador
https://orcid.org/0000-0001-5434-7550

Recibido: 15 de abril 2022
Revisado: 10 de junio 2022
Aprobado: ‘01 de agosto 2022
Publicado: 15 de agosto 2022

Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas
Año VII. Vol. VII. N° 2. Edición Especial. 2022-II
Hecho el depósito de Ley: FA2016000064
ISSN: 2542-3371
FUNDACIÓN KOINONIA (F.K). Santa Ana de Coro, Venezuela

RESUMEN

El objetivo general de la presente investigación fue analizar jurídicamente la responsabilidad bancaria frente a delitos informáticos. Se apoyó en la perspectiva cuantitativa, de tipo documental-bibliográfica. Esto en vista de que a partir de la revisión documental y el estudio de la realidad social observada se han logrado inferir conclusiones reflexivas por parte de los investigadores. La investigación documental es una técnica que consiste en la selección y compilación de información a través de la lectura y crítica de documentos y materiales bibliográficos, bibliotecas, bibliotecas de periódicos, centros de documentación e información. Se analizó la normativa vigente, tesis y trabajos arbitrados relacionados al tema en estudio. Se concluye que, Ecuador ha dado los primeros pasos en el desarrollo de iniciativas que permiten la investigación y sanción de los delitos informáticos, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados.

Descriptores: Protección de datos; banco; cibercrimen. (Palabras tomadas de Tesauro UNESCO).

ABSTRACT

The general objective of this research was to legally analyze banking liability for computer crimes. It was based on a quantitative, documentary-bibliographic perspective. This in view of the fact that from the documentary review and the study of the social reality observed, reflective conclusions have been inferred by the researchers. Documentary research is a technique that consists of the selection and compilation of information through the reading and critique of documents and bibliographic materials, libraries, newspaper libraries, documentation and information centers. The current regulations, theses and refereed works related to the topic under study were analyzed. It is concluded that Ecuador has taken the first steps in the development of initiatives that allow the investigation and punishment of computer crimes, however, it is necessary to develop, improve and implement mechanisms that allow such investigations to be developed within regulated frameworks.

Descriptors: Data protection; bank; cybercrime; cybercrime. (words takenfrom UNESCO Thesaurus).

INTRODUCCIÓN

En el año 2021, la superintendencia de bancos y la fiscalía general del Estado, remitieron resoluciones interinstitucionales, en el que obliga a toda institución financiera, en este caso, las entidades bancarias, brindar seguridad a favor de sus clientes y evitar que sean víctimas de los delitos informáticos.

En este sentido la Constitución de la República del Ecuador. (2008), indica en su artículo lo siguiente:

> Articulo. 11.- El ejercicio de los derechos de los ciudadanos y ciudadanas ante las autoridades competentes se regirá, entre otros principios, en base a que ninguna norma jurídica podrá restringir el contenido de los derechos ni de las garantías constitucionales; los principios y los derechos son inalienables, irrenunciables, indivisibles, interdependientes y de igual jerarquía; y que el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución.

En el año 2020 entre los meses de enero y agosto, según datos de Fiscalía General del Estado del Ecuador, se registró 548 denuncias a escala nacional. Es decir que los delitos más comunes tienen que ver con la suplantación de identidad, falsificación y uso de documentos falsos y apropiación fraudulenta por medios electrónicos. De igual sentido, mediante un informe de Interpol, publicado en agosto de 2020, en el mundo, el 59% de las ciberamenazas corresponde a estafas por internet y phishing; y el 36% a software malicioso.

Con respecto a la suplantación de la identidad de una persona para obtener claves de acceso para obtener información confidencial, datos sensibles, datos que están en redes sociales o entidades bancarias, hoy en día se escucha mucho a personas denunciar delitos de suplantación de identidad frente a una identidad bancaria y la mayoría de veces por no decir en su totalidad no se les ha sido resuelta o simplemente su caso quedo en “archivos”, viéndose afectado el usuario.

Se plantea como objetivo general analizar jurídicamente la responsabilidad bancaria frente a delitos informáticos.

METODOLOGÍA

La presente investigación se apoya en la perspectiva cuantitativa, de tipo documental-bibliográfica. Esto en vista de que a partir de la revisión documental y el estudio de la realidad social observada se han logrado inferir conclusiones reflexivas por parte de los investigadores, de la problemática planteada. Según Baena (1985), la investigación documental es una técnica que consiste en la selección y compilación de información a través de la lectura y crítica de documentos y materiales bibliográficos, bibliotecas, bibliotecas de periódicos, centros de documentación e información. En este sentido se analizó la normativa vigente, tesis y trabajos arbitrados relacionados al tema en estudio.

RESULTADOS

Al momento que hacemos uso de la Internet, estamos permitiendo que el mundo se mueva de manera rápida, pero eso no implica que sea seguro, ya que conforme hacemos uso de los medios de comunicación, este avanza y nos encontraremos frente a conductas delictivas que usan este medio para cometer diversas clases de delitos; es por eso que el avance de la tecnología de una manera u otra hace que la información del mundo en sí, quede almacenada en computadores. (Laptops, Tablet, etc.) Así mismo queda almacenada en bases de datos, pendrive; que toda vez que sea transmitidas por medios de comunicación, como lo es el Internet, cuyo uso del mismo es de manera infinita, incluso en el ámbito industrial, comercial, bancario. (Martínez Padilla, 2015)

Para dar a conocer la relevancia de los delitos informáticos o ciberdelitos que hoy en día nos concierne y la serie de riegos que conlleva navegar en la web mediante la utilización de las Tecnologías de la Información y Comunicación, desde aquí en adelante conocidas como las TIC, herramientas esenciales y de uso frecuente de los ciberdelincuentes para ejecutar sus actos delictivos; los usuarios frecuentes de estos medios, cada vez que pensamos en los famosos delitos informáticos se nos viene a la cabeza el fantasma de Hacker, como el peligroso delincuente que anda navegando por la red cometiendo sus infracciones; para poder prevenir y sancionar este tipo de

conductas ilícitas que afectan los sistemas y datos informáticos, secretos de comunicaciones, al patrimonio, la fe pública, la libertad sexual, entre otros, debemos saber que los ciberdelincuentes se escudan en el anonimato para cometer estos actos típicos, antijurídicos y punibles; para conocer y entender un poco más de este mundo del crimen cibernético, es importante saber de su historia, cómo se han ido desarrollando y evolucionando hasta la presente fecha (Meléndez, 2018).

En la actualidad, no existe un consenso global con relación a este tipo de conductas ilícitas, tanto en el ámbito de derecho como en la criminología. La ausencia de una definición específica se demuestra a partir de las diferentes denominaciones que reciben este tipo de conductas, “delitos informáticos”, “crímenes cibernéticos” “delitos relacionados con computadoras” “delitos electrónicos”, “crímenes por computadoras”, “cibercrimen”, “delitos telemáticos”, entre otros (Sain, 2012, p.11).

La sociedad tiene que culturizarse acerca de la nueva era digital porque los delitos cibernéticos de los cuales hablamos se diferencian en:

- Delitos Informáticos,
- Delitos Computacionales, y
- Delitos Electrónicos.

Delitos Informáticos

Son aquellos que afectan la información y al dato como bienes jurídicos protegidos, es decir, la información que un usuario tiene dentro de una cuenta de correo electrónico y el dato protegido de una cuenta bancaria, los datos que se contienen en un celular, los datos que se contienen en el sector público o privado, la identidad de ciertas personas que están protegidas por el Estado y la ley (Meléndez, 2018).

En el Ecuador los delitos informáticos son actividades ilícitas, aquellas que se comete a través de medios y dispositivos tecnológicos y de comunicación, cuyo objetivo es causar algún daño, provocar pérdidas o impedir el uso de sistemas informáticos. Todas estas actividades que contemplen, grabaciones y fotografías sin consentimiento o autorización legal, suplantación de claves electrónicas, daños o

pérdida de información intencional, intervención o violación en la intimidad de las personas, entre otras, son ilícitas (Ramírez, 2017).

Delitos Computacionales

Vienen a ser los delitos tradicionales con la implementación de la tecnología para la consumación de estos, como el robo, el hurto, la defraudación, la estafa. Por ejemplo, la estafa opera cuando el ciberdelincuente envía páginas idénticas a la de un Banco, para que ingrese su correo, usuario, contraseña, además de datos relevantes del mismo, por ese motivo es necesario que la sociedad sepa, conozca sobre estos medios de estafa electrónica para evitar este tipo de redes criminales (Meléndez, 2018).

Delitos electrónicos

Estos delitos utilizan la informática como objeto del ataque o como el medio para cometer otros delitos, frecuentemente de carácter patrimonial, como estafas, apropiaciones indebidas, entre otros. Y como un dato relevante, podemos aducir que no todos los delitos pueden ser considerados o clasificados como delitos informáticos por el mero hecho de haber utilizado un computador, un celular, una Tablet, iPad u otro medio tecnológico, para esto es indispensable precisar que conductas pueden ser consideradas como delitos informáticos y cuáles no, por ejemplo: calumniar a una persona a través de medios de comunicación, correo electrónico, mensajes de texto, mensajes vía WhatsApp, Facebook, twitter u otro medio conocido como redes sociales, estaría frente a un delito de ejercicio de acción privada, de acuerdo a nuestra legislación, se encuentra tipificado en el Código Orgánico Integral Penal.(2014) en su artículo. 182

Los delitos informáticos han ido en aumento en Ecuador, se indica en un informe publicado por EL UNIVERSO en el 2020. En el 2017 se registraron 8.421 casos; subieron a 9.571 y 10.279 en 2018 y 2019. Estas son las cifras de las denuncias. La tendencia se mantiene. Dentro de este artículo se menciona que los más recurrentes

son las estafas digitales con modalidades como la suplantación de la identidad y la apropiación fraudulenta a través de medios electrónicos. (El Universo, 2021).

Importancia de la responsabilidad bancaria dentro de los delitos informáticos

Los servicios electrónicos, que pueden implicar la utilización de hardware o software, son usualmente utilizados por estas entidades a fin de agilizar las transacciones, ahorrar personal empleado por el banco y descongestionar sus instalaciones, entre otros beneficios. Pero a la vez pueden provocar, si no se guardan las debidas diligencias de seguridad, efectos no deseados por el cliente, resultando en perjuicios económicos para él. En este contexto, el cliente se enfrenta a nuevas modalidades para operar con el banco que hasta hace poco no eran las habituales, con nuevas formas de transigir y nuevos servicios informáticos (Gallasso, 2010), considera que la importancia del tema radica en determinar en qué casos debe hacerse responsable el banco por los perjuicios sufridos por los clientes, unificar el criterio por el cual se determina la responsabilidad de los bancos frente a los fraudes cometidos por la utilización de estos servicios informáticos y también especificar qué información y de qué manera se debe proporcionar al cliente a fin de que éste también cumpla con su parte y sea responsable.

Modalidades de delitos informáticos en el Ecuador que afectan a la banca que han sido recogidos por el código integral penal. En el COIP se han tipificado delitos informáticos no solo buscando la protección de derechos constitucionales y bienes jurídicos conocidos tradicionalmente, como es por ejemplo el derecho a la propiedad, sino también el derecho de información, que se lo cataloga como un “derecho del buen vivir”.

DISCUSIÓN

La responsabilidad bancaria frente al delito informático

El artículo 308 de la Constitución de la República. (2008) establece. - Actividades, finalidad, prohibiciones y responsabilidad del sistema financiero. - Las actividades financieras son un servicio de orden público y podrán ejercerse previa autorización del

Estado, de acuerdo con la ley; tendrán la finalidad fundamental de preservar los depósitos y atender los requerimientos de financiamiento para la consecución de los objetivos de desarrollo del país. Las actividades financieras intermediarán de forma eficiente los recursos captados para fortalecer la inversión productiva nacional y el consumo social y ambientalmente responsable. El Estado fomentará el acceso a los servicios financieros y a la democratización del crédito. Se prohíben las practicas colusorias, el anatocismo y la usura.

Los bancos son responsables ante sus clientes por los contratos que celebran con ellos, por lo que responden por la inejecución o defectuosa ejecución de las operaciones a las que se compromete; pero también es responsable ante sus usuarios por los actos efectuados por sus dependientes (Villegas, 2005).

Asimilando el tema en análisis a la responsabilidad bancaria ante los robos de cajas de seguridad; La cuestión gira en torno al nivel de la diligencia exigible a la entidad de crédito y más en torno a si el robo es un suceso que entra en la esfera del riesgo de la actividad bancaria…hoy en día el debate encuentra su máxima expresión en si el robo con empleo de la tecnología más moderna merece o no el calificativo de insuperable lo que exoneraría al banco de toda responsabilidad. El robo se ha desarrollado con tal magnitud de adelantos técnicos y científicos que hace imposible en todo caso, que la entidad de crédito hubiera podido evitarlo por más esfuerzo que hubiera puesto en el empeño. (Rubio, 2012, p. 224).

CONCLUSIONES

Ecuador ha dado los primeros pasos en el desarrollo de iniciativas que permiten la investigación y sanción de los delitos informáticos, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte de los entes y profesionales dedicados a su investigación. Es importante para dar a conocer que en el país existe un problema muy grave que está afectando a los usuarios, todo esto producto de los delitos informáticos el cual se ve

reflejado tanto por la inseguridad informática que existen, así mismo por la falta de conocimiento de las personas sobre este problema.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A la Universidad Regional Autónoma de los Andes; por motivar el desarrollo de la Investigación.

REFERENCIAS CONSULTADAS

Asamblea Nacional Constituyente de la República del Ecuador, (2008). Constitución de la República del Ecuador. [Constitution of the Republic of Ecuador]. Montecristi. Registro Oficial 449 de 20-oct-2008. Recuperado de https://n9.cl/sia

Asamblea Nacional de la República del Ecuador. (2014). Código Orgánico Integral Penal [Comprehensive Organic Criminal Code]. Recuperado de https://n9.cl/g6sc

Baena, G., (1985) Instrumentos de Investigación. [Research Instruments]. Editores Mexicanos Unidos, S.A. México

EL UNIVERSO. (4 de agosto de 2021) Conozca cuáles son los delitos informáticos con pena de prisión en Ecuador. Los delitos informáticos han ido en aumento en Ecuador. [Learn which computer crimes are punishable by imprisonment in Ecuador. Computer crimes have been increasing in Ecuador]. EL UNIVERSO. https://n9.cl/1gnp8

Gallasso, M. L. (2010). La Responsabilidad Bancaria Frente A Fraudes Cometidos Por El Uso De Los Servicios Informáticos. [Bank Liability for Fraud Committed Through the Use of Computer Services]. Tesis de Grado. Universidad Empresarial Siglo 21. Cordoba, Argentina. Recuperdo de: https://n9.cl/cev13

Meléndez Verdezoto, J. (2018). Delitos informáticos o ciberdelitos. [Computer crimes or cybercrimes). Recuperado de: https://n9.cl/wqtp9

Ramírez, R. (27 de diciembre de 2017). Delitos informáticos establecidos en el COIP y cómo prevenirlos. [Computer crimes established in the COIP and how to prevent them]. Policía Nacional del Ecuador. https://n9.cl/5hpqq

Rubio, J. A. (2012). Derecho de Obligaciones. [Law of Obligations]. Obra Jurídica Enciclopédica, México: Editorial Porrúa.

Sain, G. (2012). Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet. [Crime and new technologies: fraud, drug trafficking and Internet money laundering]. Editorial del Puerto. Primera Edición. Ciudad Autónoma de Buenos Aires: Del Puerto. Recuperado de: https://n9.cl/5oi9j

Villegas, C. G. (2005). Contratos Mercantiles y Bancarios. [Commercial and Banking Contracts]. Tomo I. Buenos Aires.