Responsabilidad De Entidades Financieras: Por Falencias En El Tratamiento De Datos Personales Y Los Delitos Informáticos[1]

María José García Rivera[2]

Cristian José Pineda Rodríguez[3]

Resumen: El presente artículo de revisión nace con el fin de exponer a la colectividad colombiana la importancia actual que representan los datos personales, por las nuevas modalidades y métodos para sustraer información, dinero u otros activos por medio de dispositivos electrónicos, denominados; los delitos informáticos.

De esta forma, se planteó el objetivo general: describir el tipo de responsabilidad en las que incurren las entidades financieras que prestan servicio en Colombia, frente al mal tratamiento de datos personales. Y si existen vacíos para la aplicación del tipo penal en delitos informáticos. El presente estudio se realizó desde un modelo de tipo cualitativo, ya que la pretensión radica en estudiar toda la información bibliográfica que aporte en la búsqueda de la respuesta a la pregunta planteada. Así mismo, el diseño de investigación es de tipo documental, biográfico. Como resultado se evidencia que tienen facultad sancionatoria la Superintendencia de Industria y Comercio y la Superintendencia Financiera, siendo de carácter administrativo y en cuanto a la responsabilidad penal, se logró denotar que no se sanciona penalmente a personas jurídicas, es una responsabilidad individual, de igual modo se detectan vacíos en los tipos penales respecto de los delitos informáticos, y se detectan las obligaciones a las que están sujetas las entidades para su protección.

Palabras Claves: Delitos Informáticos; Protección de Datos; Habeas Data; Entidades Financieras; Ciberdelitos; Responsabilidad.

---

[1] Artículo de Revisión Bibliográfica para obtener el Título Profesional de Abogado. Asesor Metodológico: Laura Victoria Cárdenas Rojas, Asesor Temático: Dany Steven Gómez Agudelo.

[2] Estudiante de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Luis Amigó.
Correo: Maria.garciaiv@amigo.edu.co

[3] Estudiante de la Facultad de Derecho y Ciencias Políticas de la Universidad Católica Luis Amigó.
Correo: Cristian.pinedaro@amigo.edu.co

Abstract: This review article was born in order to expose to the Colombian community the current importance represented by personal data, by the new ways and methods of subtracting information, money or other assets through electronic devices, called; cybercrime.

In this way, the general objective was raised: to describe the type of responsibility incurred by the entities providing services in Colombia, in the face of the misuse of personal data. And if there are gaps in the application of the criminal type in cybercrime. This study was carried out from a qualitative model, as the claim lies in studying all the information literature to contribute in the search for the answer to the question posed. Likewise, the research design is documentary, biographical. As a result, it is evidenced that the Superintendency of Industry and Trade and the Financial Superintendency have the power to sanction, being administrative in nature and in terms of criminal responsibility, it was possible to denote that no legal persons are penally punished, it is a individual liability, similarly, gaps in criminal rates are detected in respect of cybercrime, and the obligations to which entities are subject for protection are detected.

Key words: Computer Crimes; Data Protection; Habeas Data; Financial Institutions; Cybercrime; Responsibility.

Introducción

El tema a tratar en el presente artículo de revisión bibliográfica es sobre los delitos informáticos y la importancia de los datos en la era de la cuarta revolución industrial, donde la digitalización se ha vuelto un factor clave para enfrentar los nuevos retos del siglo y ha llevado a que todos los procesos de la vida diaria se digitalicen, lo que toma mayor relevancia durante la contingencia por el Covid 19, toda vez que las personas están sometidas por completo al uso de la tecnología siendo más propensos a nuevas formas de delitos, que son: los delitos informáticos, donde los crackers y piratas informáticos utilizan diferentes modalidades para sustraer información, dinero u otros activos por medio de dispositivos electrónicos.

Por ende, la pregunta de investigación consiste: ¿Cuál es el tipo de responsabilidad en las que incurren las entidades financieras que prestan servicio en Colombia, frente al mal tratamiento de datos personales?

De acuerdo con lo anterior, el articulo tuvo como objetivo general:

Describir el tipo de responsabilidad en las que incurren las entidades financieras que prestan servicio en Colombia, frente al mal tratamiento de datos personales. Y si existen vacíos para la aplicación del tipo penal en delitos informáticos.

Mientras que se plantearon los siguientes objetivos específicos:

- Identificar el origen y la noción de los datos, igualmente sus normas en el ordenamiento Colombiano, así mismo las posibles falencias respecto a la responsabilidad penal en los delitos informáticos.

- Analizar el principio de circulación de los datos personales y qué métodos de protección utilizan los bancos.

- Mencionar las obligaciones y sanciones a las que están sujetas las entidades financieras.

Por otra parte, el tipo de investigación en el presente trabajo es un artículo de revisión debido a que:

> El artículo de revisión es considerado como un estudio pormenorizado, selectivo y crítico que integra la información esencial en una perspectiva unitaria y de conjunto. Es un tipo de artículo científico que sin ser original recopila la información más relevante de un tema específico. Su finalidad es examinar la bibliografía publicada y situar en cierta perspectiva (Carrasco, 2018, p.1)

El modelo de investigación es de índole cualitativo, ya que se estudió y analizó información bibliográfica que permitió dar respuesta a la pregunta de que se planteó e igualmente su diseño de tipo documental, biográfico. Las fuentes de información son de carácter bibliográfico tales como investigaciones, tesis de grado, artículos de revista indexada, informes, libros que tienen relación con el tema en mención.

Finalmente, el trabajo se ha de componer de tres capítulos y un acápite final de conclusiones. En el primer capítulo, se identifica el origen y la noción de los datos, igualmente sus normas en el ordenamiento Colombiano, así mismo las posibles falencias respecto a la responsabilidad penal en los delitos informáticos. En el segundo capítulo, se analizó el principio de circulación de los datos personales y qué métodos de protección utilizan los bancos. Por último, se menciona las obligaciones y sanciones a las que están sujetas las entidades financieras.

I. Noción De Datos En El Ordenamiento Colombiano Y Las Falencias En La Responsabilidad Penal.

El mundo moderno se caracteriza por la utilización de medios informáticos o sistemas de información, como lo define O'Brien, James (2001) "Un sistema de información es una combinación organizada de personas, hardware, software, redes de comunicaciones y recursos de datos que reúne, transforma y disemina información en una organización" (Citado por Prieto & Martínez, 2004, p. 3), es por esto que se han causado una serie de fenómenos culturales, políticos, económicos, trayendo consigo una serie de avances y a la vez riesgos.

Así mismo, es que los datos personales de la población en general han pasado de estar en pilas de papeles, archivadores u otros sitios donde reposaban, a estar en servidores[4] o en su defecto

[4] Un **servidor** es una aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

a estar almacenada en la nube[5], todo esto a través de la conexión de internet, que ha tenido una evolución notable durante estas últimas décadas, en medio de una guerra fría la cual comenzó en:

> Octubre de 1957, con el lanzamiento al espacio del primer satélite soviético, el Sputnik, y EE. UU. en 1962 con el objetivo de crear una red militar de telecomunicación y solo hasta el año 1966 se utilizó el término "paquete", por primera vez, definiéndolo como "un sistema de almacenamiento y envío de mensajes cortos" (Aldania, 2004 pp. 322-337)

Su evolución fue continuando hasta la era actual donde esos sistemas de almacenamiento, servidores y sistemas de conexión ha tenido un esparcimiento a nivel mundial rigiéndose por la vida diaria de los seres humanos, encontrándose información personal de las personas en repositorios, bases de datos, carnet de identificación, celulares, discos duros u otro dispositivo donde se genere almacenamiento.

Es por ello, que en la actualidad ya se habla sobre Macrodatos o (Big Data) cuyo concepto de Macrodatos hace "referencia a un sistema de gestión de la información, en particular de grandes volúmenes de ella generados en ambientes digitales o ecosistemas de medios digitales" (Aristizábal, 2019, p. 20). Todo esto ha generado que los estados como garantes de la protección de la intimidad, acuden a los origines, la Declaración Universal de los Derechos Humanos cuyo artículo que reza así:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. (Asamblea General de Las Naciones Unidas, 1948, p.26).

Por ello el Estado colombiano en la constituyente del año 1991 estableció en la parte dogmática[6] de la Constitución Política de Colombia, como un derecho fundamental, donde consagra el Artículo 15:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las

[5] La computación en la nube es la disponibilidad a pedido de los recursos del sistema informático, especialmente el almacenamiento de datos y la capacidad de cómputo, sin una gestión activa directa por parte del usuario.

[6] Pues bien, por la parte dogmática de la Constitución (de las constituciones), se habla de aquella parte que consagra valores superiores de una sociedad, que postula los principios y fines estatales, y las libertades a proteger principalmente por el ordenamiento jurídico. En síntesis: se trata de un conjunto de normas que establecen los principios básicos que orientan la vida del Estado y los derechos de las personas.

> informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. (Const.,1991, art. 15).

Sirviendo como faros orientadores de cómo debe ser la protección de los datos, surge la necesidad de leyes que regulen, ante esto nace la Ley 1851 de 2012, en la que se dictan disposiciones generales para la protección de datos personales, que materializa este principio constitucional, que abarca el artículo 15 y al mismo tiempo el artículo 20, el derecho a la información y a ser informado. De igual modo, da definiciones en un sentido amplio de la terminología empleada, quiénes son los sujetos, como opera la información, cuál es el titular de la información, que datos son privados o públicos y cuáles son los principios que rigen la protección de los datos, etc.

Por concepto de dato personal, lo define la Superindustria como aquella información asociada al contexto personal de ciudadano, que se encuentre asociado a su estado civil, trayectoria académica, laboral, profesional, etc.… y de igual modo, trata datos más sensibles como las características físicas, afinidad a partidos políticos, inclinaciones sexuales, etc. (Superintendencia de Industria y Comercio, *s.f.a)*

Por tanto, estos datos tienden a dividirse en tres tipos que la Superintendencia de Industria y Comercio *(s.f.b)* los clasifica en, Datos privados, Semiprivados y los Datos Públicos, que sirven para jerarquizar el grado de protección, tratamiento y almacenamiento de estos.

Ahora, entiéndase como "Dato privado: "Aquel que por su naturaleza íntima o reservada sólo es relevante para el Titular" (Ley 1266, 2008, art.3). Estos tienen una connotación especial y solo podrían ser empleados "con el consentimiento del titular, por orden de autoridad judicial en el cumplimiento de sus funciones, para salvaguardar la vida de la persona, cuando tengan finalidad histórica o estadística. (Superindustria, *s.f.b)*

En segundo lugar, encontramos los:

> **Datos Semiprivados** que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios. (Ley 1266,2008, art. 4)

Por último, están los datos públicos que la ley 1266 (2008), los califica, aquellos que la norma jurídica o constitución no les da el carácter de los antes mencionados y su contenido se

encuentra en documentos públicos, sentencias ejecutoriadas que no tengan carácter de reserva y el estado civil de las personas, estos datos se vuelven de interés general y público conocimiento.

En este orden de ideas, en el compendio de leyes creadas para la protección de datos personales existe la Ley 1266 de 2008 (habeas data) enmarcada en el derecho constitucional del cual deben gozar todas las personas de conocer, rectificar y actualizar la información que repose en bases de datos.

Es posible determinar según los parámetros de la ley quienes son los sujetos facultados para intervenir en los procesos de almacenamiento, recolección y difusión de la información siendo uno de estos según el artículo 3° de la presente ley, como la fuente de información:

> Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. (Ley 1266, 2008, p. 1).

En el marco legal, acudiendo al artículo 8° establece unos deberes a las fuentes de información, donde hay un requisito general llamado autorización, del cual emana o debe ser proporcionado por el titular de los datos personales, es decir; debe ser este sujeto el llamado a dar su consentimiento, conocer cuál es la finalidad de las entidades financieras a la hora de recolectar la información , el numeral 5 establece:

> Solicitar, cuando sea del caso, y conservar copia o evidencia de la respectiva autorización otorgada por los titulares de la información, y asegurarse de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado, cuando dicha autorización sea necesaria (Ley 1266, 2008, p. 1)

Es por ello, que ha surgido la necesidad de desarrollar múltiples instrumentos de carácter normativo cuyo fin está encaminado a asegurar el respeto y la integridad de todas las personas, esto indica el alto nivel de importancia social que adquiere los datos a la hora de desarrollar la vida en sociedad, es decir las actividades humanas, donde hay una entrega constante de información.

La tasa de Cibercrímenes ha ido en un aumento exponencial, donde los afectados en estos casos son las empresas y usuarios, como consta el informe sobre las Tendencias del Cibercrimen,

> El impacto que sufren las empresas colombianas luego de un ciberataque trasciende el coste económico por pérdidas de sus activos financieros y conlleva de manera colateral afectaciones a la productividad, daños

> reputacionales e incluso implicaciones de carácter legal por fuga de información privilegiada y data sensible. (Policía Nacional de Colombia [PONAL],2019, p.4).

Los últimos datos reportados por la Fiscalía y la Policía Nacional, indican cuáles son las modalidades y también brinda una estadística sobre el tema, resaltando las cifras más recientes frente a las modalidades, y la cantidad de personas que se han visto afectadas por los delitos informáticos.

En contexto, la Fiscalía General de la Nación (2018), brindó un reporte sobre el incremento desde el año 2017, al 2018 ha sido de un 68.5%, donde el primero reportó 9.011 denuncias y el último 15.181. La mayor concentración es en las grandes ciudades, como Bogotá, Medellín y Cali, donde la modalidades más utilizadas son; phishing: ingeniería social, clonación de tarjetas, retenedor físico, cambiazo, pagos en línea de bienes y servicios, uso de software malicioso (*malware),* ante esto la Fiscalía General de la Nación, (2018), data de estos *modus operandi*[7], donde se detecta que los delitos informáticos que más se comenten son: "Hurto por medios informáticos y semejantes: 8.817 denuncias, Violación de datos personales: 2.180 casos y acceso abusivo a un sistema informático: 2.005 denuncias[8] (p.13).

En un informe más actual de tendencias del Cibercrimen en Colombia, datan que para el año 2019, por el canal que dispone la Policía Nacional de Colombia, (2018) para la atención al ciudadano y empresas, hicieron un reporte de 28.827, de lo cual solo se hicieron efectivas 15.498 denuncias.

La Policía Nacional de Colombia (2019), identificó que el principal interés es monetario y el robo de identidad, clasificando en las dos primeras posiciones a hurto por medios informáticos y violación de datos personales, como las mayores amenazas a personas y empresas, ya que la primera cuenta con 31.058 casos y la segunda con 8.037.

Es por lo que Colombia mediante la creación de la Ley 1273, (2009) nace un nuevo bien jurídico tutelado, denominado "De la protección de la información y los datos", producto de esto, se crea nuevos tipos penales que regulan los delitos informáticos y la protección de la información.

[7] Expresión latina que significa 'modo de obrar' y se usa para referirse a la manera especial de actuar o trabajar para alcanzar el fin propuesto.
[8] (Fiscalía General de la Nación, 2018) *ibidem*

Con antelación se había llevado a cabo la celebración del convenio sobre la Ciberdelincuencia y en ella se expresó en el preámbulo “Preocupados por el riesgo de que las redes electrónicas y la información electrónica sean utilizadas para cometer delitos y que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes” (Council of Europe,2001, p, 2)

En primer lugar, la implementación de la Ley 1273 del 2009 implicó cambios en el ordenamiento jurídico Colombiano y generó la creación de nuevos tipos penales denominados “de la protección de la información y de los datos” donde se anexan 10 tipos penales reunidos en dos capítulos: Cuyo primer capítulo consta de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, que va del Artículo **269A** al **269H,** y el capítulo segundo referente de los atentados informáticos y otras infracciones, cuyos artículos rezan en los Artículos **269I** al **269** (Ley 599,2000).

A) Falencias En El Tipo Penal

Una vez se identifican los cambios de tipo normativo que fueron adicionados al código penal con el fin de sancionar los delitos que atenten contra un nuevo bien jurídico tutelado de los datos y la información, se avizora que fuera de existir una pena para quien incurra en ello también acarrea una sanción de tipo económico con un monto bastante alto.

Sin embargo, el tema de la creación de nuevas leyes es tan solo una de las muchas medidas que se deben adoptar, es allí donde toma importancia es la verdadera aplicabilidad de las leyes, es decir, que se cumpla con lo que allí se consagra y opere de manera eficaz e eficiente.

El avance para reducir el índice de infracciones de delitos informáticos se puede aducir a la creación de leyes como la 1273 del 2009, aunque como lo ha expuesto:

> Kevin Mitnick, experto en seguridad informática, considera la normatividad positiva, debe evolucionar y adaptarse al compás de la tecnología, día tras día las tendencias y sistemas cambian, mejoran y evolucionan, entonces las leyes se van quedando obsoletas, Mitnick estadounidense que fue encarcelado durante 5 años por delitos informáticos, se dedica en la actualidad a burlar la seguridad de grandes empresas para después elaborar sistemas seguros, ya desde la legalidad. Citado por (Buitrago, 2015, p.11)

Podría considerarse que el reto para la legislación Colombiana en materia de delitos informáticos es reformar la estructura en la cual están redactados determinados artículos los

cuales están consagrados específicamente en la ley 1273 del 2009, esto con el fin de no permitir la materialización de las nuevas conductas delictivas, toda vez que los vacíos o la falta de clasificaciones claras y precisas sobre los delitos informáticos, pero mucho más importante que esto es la ausencia de claridad en los medios utilizados por los infractores para cometer un ataque delictivo permitiendo así que, se atente contra la confidencialidad de la información tanto de carácter personal como financiero de un sujeto o de una colectividad.

De conformidad con lo dicho anteriormente existe una falencia bien sea de carácter conceptual o en su defecto de aplicabilidad, más concretamente en el artículo *269G-*,

> "Suplantación de sitios web para capturar datos personales":
> 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 (Ley 1273,2009, art 269G)

Este artículo al indicar como verbos rectores tales como diseñe, desarrolle, trafique, venda, ejecute, programe o envíe, no alcanzan a ser suficientes a la hora de imputar o acusar respecto de estos delitos informáticos, al momento de presentarse una situación fáctica, un ejemplo:

> El spam puede considerarse como delito informático, esto pensado cómo a través de este medio se puede filtrar muchas veces correos que no propiamente son basura y que por el contrario son enviados con el fin de apoderarse de algún tipo de información confidencial de la víctima y de esta manera atentar contra la privacidad e incurrir en otro delito aún más grande llegando a la estafa, falsificación, entre otros. (Castillo,2017, p. 82)

Ahora bien, si en los tipos penales existen inconsistencias para regular los delitos informáticos de forma tal que son ambiguos y crean confusión o peor aún vacíos jurídicos esto, ya que, a la hora de determinar la comisión de un delito informático, es casi que imposible que se judicialice correctamente a el infractor.

En relación con lo anterior, la Sala de Casación Penal de la Corte Suprema de Justicia, se enfrentó ante una problemática en cuanto a los tipos penales de los delitos informáticos que carecen de exactitud, toda vez que para la creación de los delitos relacionados con la protección de la información y los datos personales, se tomó la escritura de otros tipos penales que son

análogos, causando esto una interpretación errada por parte de quien juzga y además dejando carencias estructurales en los tipos penales, generando ello de alguna forma ineficacia más precisamente en el caso del Hurto por Medios Informáticos:

> Se trata de un tipo penal de naturaleza claramente subordinada y compuesta. En efecto, la descripción normativa, en su tipo objetivo positivo y en la consecuencia jurídica, no consagra la conducta reprochada, el objeto material, ni la sanción correspondiente, sino que, en cuanto se refiere al comportamiento antijurídico y al referido objeto sobre el que recae la acción prohibida, efectúa un reenvío normativo al tipo base de hurto (artículo 239 de la Ley 599 de 2000) y a la disposición que lo califica (canon 240 ejusdem) para determinar la sanción imponible. (Corte Suprema de Justicia, Sala de Casación Penal, SP 1245-42724, 2015)

En dicho concepto la sala de casación penal establece varios elementos constitutivos del tipo penal consagrado en el artículo 269I del Código Penal, que son relevantes a la hora de establecer responsabilidad, ya que el hurto por medios informáticos y semejantes es un delito de resultado, ya que requiere como lo indica el mismo artículo que se efectúe un menoscabo real al patrimonio económico de una persona.

Respecto a la responsabilidad penal, donde hay una dicotomía entre, sí es un delito empresarial o si es un delito dentro ejecutado por un empleado, por ende se ha notado que en Colombia crean sociedades con el fin de cometer actos fraudulentos, donde camuflan su actuar, ya que "la normatividad vigente, no contempla sanción penal alguna para el actuar delictivo de la persona jurídica, y esto constituye un vacío normativo, que fomenta la impunidad y la posterior comisión de más delitos que afecten la seguridad jurídica del Estado". (Martínez, 2018, p.9).

Al no estar estipulada la tipología penal de las personas jurídicas, se concluye, que quien realice la acción responderá por su actuar, condenando el acto y que cada actuación será llevada por el órgano competente y se evaluará cada caso en particular.

A la hora de establecer la responsabilidad penal en materia de delitos informáticos existen factores relevantes que menciona la Corte Suprema de Justicia, mediante Sentencia (SP 1245-42724, 2015), es el resultado ya que se requiere de una materialización de los efectos que causa la conducta punible, por ejemplo, en la comisión del hurto informático es indispensable que se genere un detrimento real en el patrimonio de una persona.

Por ende, se ha de remitir a la Ley 1273 de 2009, donde se adiciona el nuevo bien jurídico tutelado, por lo que se ha de investigar y juzgar individualmente a quien lo ejecute; sea autor,

coautor, participe, cómplice o si se realiza un concierto para delinquir. Asimismo, se ha de estudiar cada caso en particular para estipular el tipo penal de los que concierne a "la protección de la información y los datos" de igual forma identificar bajo que modalidad actuó, por parte del ente investigador.

Además, se identifica una característica de los delitos informáticos frente a la punibilidad, que las penas oscilan entre 48 y 96 meses y multas de 1.000 SMLMV, conforme a la Ley 599 del 2000. Aunque, hoy en día la normativa se va quedando algo corta en cuanto las modalidades de la comisión que se han renovado, ya que con el pasar de los años los medios digitales cambian y conforme a la tipificación, se presentan vacíos; como no determinar el sujeto que la realiza, solo está cargada de verbos rectores, pero en si no determina una conducta específica; por consiguiente, habría que modificar y especificar la conducta, para así poder atribuir una violación a la ley.

Es decir, al formarse vacíos o lagunas jurídicas, la interpretación de un tipo penal de delito informático no se presenta como tarea fácil para quienes administran justicia, al no haber una tipificación adecuada y de igual modo incurriendo en la vulneración de derechos, tanto para quien se presume que comete el ilícito, ya que muchas veces pueden imputar delitos que no cometió, por el vacío normativo, por otra parte la víctima de un delito informático, se puede ver vulnerada, toda vez que su caso puede quedar en la impunidad, por la dificultad probatoria en estos casos y que así puedan generar una condena., puesto que hay una gran dificultad en llegar a quien cometió el tipo, toda vez que hay un gran automatismo involucrado en este tipo de delitos, por ello, esto separa temporalmente al autor del hecho, que fácilmente podría estar físicamente en otro lugar, imposibilitando construir una relación directa entre el ataque y el atacante. (Asobancaria & OEA, p.139).

Conforme a la estructuración, que es altamente especializada y "se han detectado grupos dedicados exclusivamente a actividades como la recolección y compilación de bases de datos con datos personales"[9](p.139), ante esto, ha generado la dificultad de poder imputar o condenar estas estructuras dedicadas al hurto por medios informáticos. De igual modo, "a pesar de que habían sido detenidos los reclutadores, ninguno de ellos conocía el origen de los datos o quién había efectuado el ataque, ya que su función se suscribía exclusivamente al retiro en efectivo de los

[9] *Ibidem (Asobancaria & OEA)*

activos robados", estas personas son conocidas como "*Money Mules",* es por ello, que las estructuras de estas organizaciones, ha de dificultar la responsabilidad a una persona en particular.

En relación con las dificultades a la hora de aplicar una sanción idónea o correspondiente ante la comisión de algunos delitos informáticos, Asobancaria & OEA (2018), considera que la eficiencia depende de asumir unos desafíos del riesgo cibernético en el sector financiero no solo para Colombia, sino también para América Latina en las entidades bancarias que hay en la región. Además, establecen que el reto principal consiste en implementar nuevas alternativas digitales con el fin de proporcionar soluciones de seguridad, para brindar una verdadera protección a los intereses de los usuarios.

En razón a ello Asobancaria, aporta estadísticas y datos que demuestran que "tan solo un tercio de los bancos implementan herramientas, controles o procesos usando Big Data.

- En promedio, más del 90% han implementado los cortafuegos y las actualizaciones automatizadas de virus y sistemas.

- Los riesgos de seguridad digital que tienen más atención para este tipo de entidades son: i) robo de base de datos crítica, ii) compromiso de credenciales de usuarios privilegiados, y, iii) pérdida de datos.

- En promedio, el 49% de las entidades bancarias no implementan herramientas, controles o procesos usando tecnologías digitales emergentes. Tan solo el 29% de las entidades han implementado soluciones de Big Data. (Asobancaria & OEA, p. 19-20).

II. El Principio De Circulación De Los Datos Personales Y Los Métodos De Protección Que Utilizan Los Bancos

Para empezar, según la Ley 1266 (2008), se encuentra consagrado el principio de circulación restringida en su artículo 4°, donde el legislador establece, que los datos deben estar regidos a la naturaleza de los mismo y que su información está sujeta a la ley, donde prima la temporalidad y finalidad del banco de datos, un claro ejemplo; los datos del usuario no deben ser accesibles para otras personas por motores de búsqueda como Google.

Los bancos ya han sido producto de sanciones por un mal manejo de los datos personales como es el caso donde la Superintendencia de Industria y Comercio (2020) sanciona a Scotiabank por el incumplimiento de la Ley 1851 de 2012, la Superintendencia a través de la Resolución 10720 manifiesta que por medio de la queja de un usuario, donde en reiteradas ocasiones le manifestó a SCOTIABANK COLPATRIA, el deseo de la supresión de su información, pero aun así seguía recibiendo mensajes, aun cuando ya había usado el mecanismo del Habeas Data. Y en la presente investigación se conoce que los datos del usuario eran producto de un convenio de ETB con Scotiabank, se ha de analizar si había una autorización expresa.

La Corte Constitucional en la Sentencia C-1011 (2008), indica que este principio está dirigido a determinar que la administración de los datos personales se sujeta a los límites que se derivan de su naturaleza, de la norma estatutaria y de los principios que le son aplicables a esa actividad. Y que se encuentra vinculado con los principios de finalidad y necesidad, donde la Corte Constitucional en la Sentencia T-020 (2014), los define, siendo el primero aquel que "suponen la existencia de un objetivo constitucional legítimo que, a su vez, delimita qué puede hacerse con el dato y *el segundo, aquel que* se refiere a que el tratamiento de dicho dato cumpla con el fin que abarca su manejo". (p.1)[10].

Además, la Superintendencia Financiera en medio de sus atribuciones legales, en ejercicio de sus facultades legales y constitucionales, emite una serie de reglamentos y directrices estipuladas en la Circular Externa 018 de 2016, donde se les prohíbe incorporar prácticas y cláusulas abusivas en los contratos realizados con entidades financieras, es por ello que la Superfinanciera Circular Externa 018 (2016) en el numeral 6.2.40, ha de establecer que no se puede mediante una sola firma, autorizar el total manejo de información personal, para que comparta información del consumidor financiero con las entidades pertenecientes a su conglomerado bancario, sin que se lleve a cabo el cumplimiento de los requisitos que establece la normatividad en materia de protección de datos personales.

Los datos se han degenerado en un instrumento de comercialización que no encuentra barreras ni fronteras de tipo territorial, todo gracias al internet, empresas o entidades financieras como fuentes de información al recolectar los datos de los usuarios, tienen presente la importancia

[10] palabras propias en cursiva.

actual que representa para el mercado. Como dijo una vez Alexander Nix “En la era digital, los datos son el nuevo petróleo” citado por (Kaiser, 2019, p.16).

Ante esto, Asobancaria (2019), plantea de cómo la “banca ha sido testigo del desarrollo vertiginoso de tecnologías innovadoras que están transformando el modelo de negocio tradicional, permeando desde el nivel operativo hasta el comercial con herramientas como la inteligencia artificial (AI), el machine learning y el Big Data” (p. 1).

Ahora el mundo se encuentra en una transformación política, económica, social, tecnológica, etc.… todo siendo producto de la cuarta revolución industrial que “es el resultado del dinamismo de las **tecnologías** y de la combinación de **sistemas digitales** y físicos para mejorar la calidad de vida del ser humano.” (Universidad Sergio Arboleda, *s.f,* p.1), y esto lo advierte Klaus Schwab en su libro “La Cuarta Revolución industrial” (2016) "Estamos al borde de una revolución tecnológica que modificará fundamentalmente la forma en que vivimos, trabajamos y nos relacionamos. En su escala, alcance y complejidad, la transformación será distinta a cualquier cosa que el género humano haya experimentado antes” Citado por Valeria Perasso de la (BBC Mundo, 2016, p.1).

El entorno de las tecnologías disruptivas lleva envuelto consigo grandes retos para el sector bancario, por eso ante esta evolución se encuentran una serie de riesgos en la prestación del servicio como “Nuevos riesgos de seguridad, mayor acceso a y uso de datos personales, riesgos de las herramientas automatizadas” (BBVA, 2017, p. 8).

Las entidades financieras no ajenas a la realidad crean o desarrollan mecanismos que generen en primer lugar captación de usuarios. Como es el caso del uso del “Clustering”, que consiste en la automatización de encontrar patrones significativos dentro de un conjunto de datos, para identificar fácilmente el patrón subyacente.” (Jaime, 2017, p. 8)

Para que las entidades financieras logren esto requieren conocer diversos tipos de información que permitan determinar patrones de preferencias en los usuarios y de esta manera brindarles lo que finalmente busca, es decir, la entidad financiera por medio de los datos personales conoce al usuario y en esa medida le proporciona comodidades o ventajas según sus necesidades.

El aspecto que se descuida o queda a la deriva no sin ser el más importante es la seguridad de los datos y esto acarrea una falta de protección y de autorización donde ha surgido un fenómeno

conocido como el comercio de datos, el cual ha llegado a traspasar las fronteras entre países, que se convierte en lo que se ha denominado la transferencia internacional de datos basada en;

> La importación o exportación de esa información de un país a otro. Esto supone que los datos se encuentran en un país y deben ser trasladados o enviados a una empresa domiciliada en otro Estado. Este fenómeno también es conocido como "movimiento internacional de datos" o "flujo transfronterizo de datos". (Angarita, 2010, p. 6)

Concerniente a lo anterior, la OECD ha hecho varios análisis de las deficiencias que se presentan en Latinoamérica, donde la OEA (2014), indica cuales deben ser los planes a mejorar, como la "creación y mejora de marcos jurídicos de seguridad digital, creación de capacidades operativas para gestionar el riesgo de seguridad, distribución clara de responsabilidades entre las instituciones gubernamentales y cooperación internacional entre múltiples partes interesadas" citado por (OECD/BID, 2016), y a su vez en el CONPES 3854 (2016) se indica las necesidad de:

> Crear las condiciones para que las múltiples partes interesadas puedan gestionar la seguridad digital de sus actividades económicas y sociales, debe fomentar la confianza en el entorno digital y, además, *(...)*; (ii) afirmar claramente que su objetivo es aprovechar el entorno digital abierto para la prosperidad económica y social. (p.26)

Entonces, en la actualidad personas y empresas han migrado a los servicios tecnológicos, es por ello por lo que, en materia de Ciberseguridad, todos los actores del proceso están en búsqueda de una política que sea más eficaz para la protección de los usuarios, donde "Finalmente, se logró reconocer que la cooperación resulta ser un aspecto fundamental para judicializar y reducir los incentivos hacia el crimen". (Asobancaria, 2018, p. 5).

A) Métodos De Protección (IA).

Ante esta inminente preocupación Asobancaria a través de [CSIRT Financiero][11] (2019), logra identificar cómo se está convirtiendo en un flagelo económico importante para la sociedad, ya que este es consecuente después de la corrupción estatal y el narcotráfico, donde Latinoamérica no ha sido ajena a esta realidad, especialmente en Colombia, donde posteriormente del CONPES

[11] (Centro de Respuesta a Incidentes de Seguridad en Tecnologías de la Información) es el equipo de respuesta de apoyo a la respuesta de incidentes del sector financiero que fomenta la colaboración de sus miembros y el intercambio de información para afrontar de manera efectiva las amenazas cibernéticas.

3855 del 2016, Asobancaria crea el grupo CSIRT, para la protección de su bien más preciado *"su información"* y donde se enfoca principalmente en cuatro aspectos:

1. Monitoreando el panorama de ciberamenazas para el sector financiero en tiempo real.
2. Desarrollando una comunidad de intercambio de inteligencia cibernética con equipos locales e internacionales especializados.
3. Estableciendo un enfoque organizado y estructural de la gestión de incidentes.
4. Mitigando el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones a través de respuestas efectivas y eficientes. (Asobancaria [CSIRT Financiero],2019, p.1)

Es importante resaltar, el papel de las organizaciones internacionales, donde se destaca el *[IIF]Institute of International Finance* (2017) *o* Instituto de Finanzas Internacionales, manifiesta que las organizaciones que prestan servicios financieros deben de preocuparse por la ciberseguridad y reinventar la forma en que los bancos gestionan el riesgo. (p.1).

Ahora, en otro apartado resalta la gran importancia de utilizar nuevos métodos para la protección de los datos, es por ello por lo que manifiestan, que:

> Los bancos dependen de las personas para implementar, mantener y proteger los sistemas y los datos. Los datos ayudarán a identificar y abordar los riesgos emergentes, así como informar las decisiones estratégicas y cotidianas. *(…)* Los bancos están adoptando nuevas tecnologías como blockchain, automatización de procesos robóticos (RPA), chatbots y más. Los encuestados esperan que las nuevas técnicas y tecnologías reduzcan los costos en la gestión de riesgos, en particular mediante el uso de automatización (87%), digitalización (64%), aprendizaje automático (59%) y modelos de riesgo que utilizan inteligencia artificial (IA) (57%).(Institute of International Finance [IIF], 2017, párr. 5)

En este orden de ideas, el MinTic (Ministerio de Tecnologías de la Información y Comunicación) en la Agenda Estratégica de Innovación del Nodo Ciberseguridad, plantean que en Colombia ya se han establecido cuales son los lineamientos básicos e igualmente manifestado cuales son los esquemas y de cómo dar la atención a estos procesos y que herramientas utilizar para que se dé oportunamente la captura de datos, el análisis, el transporte y la respuesta, ante alguna situación. (Min Tic, 2014).

Al mismo tiempo, indican desde el alto gobierno, en este caso desde el Min Tic que, la necesidad de realizar procesos innovadores que estén orientados a la integración de datos para así fomentar la interoperabilidad y se esté en capacidad de responder y prevenir. (Min Tic, 2014).

Por otra parte, la circulación restringida de los datos personales como principio rector dentro de la relación entre entidad financiera y el usuario, debe ser respetado y acatado sin excusa alguna, todo en aras de evitar que el titular pierda esa potestad que le faculta la ley para autorizar y finalmente decidir quién puede tener acceso, es así como la Ley 1266 (2008), en el artículo 4° "Principios de la administración de los datos personales " en el literal "C" indica, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que sea técnicamente controlable para brindar un conocimiento restringido sólo a los autorizados conforme a la presente ley (p.1).

De acuerdo con lo anterior, puede converger una excepción permitida solo si en términos de seguridad se implementa de forma técnica mecanismos que brinden seguridad al titular de la información, como el Cloud computing, que se componen por el flujo de datos, que concierne a personas naturales y son denominados de carácter personal y gozan de una garantía especial frente al tratamiento que otros pueden realizar con este. (Bravo, 2011, p.46)

Por lo antes expuesto queda una pregunta ¿Qué hacen los bancos frente al tema de la ciberseguridad? antes de lograr encontrar una respuesta es pertinente exponer que según:

> La Distribución Porcentual de Ataques Cibernéticos por Tipo (Fuente Reporte Anual IC3).De los ataques perpetrados durante el año 2019, el Phishing ocupó el primer lugar con un mayor número de víctimas, a las cuales se les envió correos electrónicos haciéndose pasar por empresas o entidades bancarias, con la finalidad que los usuarios facilitarán información confidencial de sus cuenta bancarias, tarjetas de crédito u otra información con la cual pudiesen obtener un lucro económico a expensa de la víctima. Este tipo de fraude electrónico representó el 25% del total de las denuncias de ciberataques mundiales. (Suárez, 2020, pp. 4-5)

Estas cifras demuestran el aumento de ciberataques y por otro las fallas que aún siguen existiendo frente a la seguridad de la información, esto no solo consiste en la compra de programas, también deben generar un índice elevado de confiabilidad, no es suficiente el dinero que se invierte para la ciberseguridad, hay otros factores no han sido valorados por parte de las entidades.

Visto que, en otros países la inversión respecto a temas de seguridad es un factor clave, como Suárez (2020), dice: "Según la investigación de Precise Security [6], la inversión en ciberseguridad a nivel mundial durante el 2019 fue de 106.600 MM$, lo que significó un incremento del 10,1% respecto al realizado el año 2018" (…) Donde dicha compañía revela que:

> "Dinamarca es el país con mayor ciberseguridad del mundo, subiendo desde el cuarto lugar que tuvo el año pasado, desplazando a Japón del sitial de honor, el cual cayó a la quinta posición. Completan la lista de los primeros 5 países de alto rendimiento: Suecia, Alemania, Irlanda y Japón" (Suárez, 2020, p.11).

Conforme a estos datos, es importante que Colombia, inicie con la implementación de mecanismos de protección para que logre posicionarse a nivel mundial como un país que apuesta por el desarrollo en materia de seguridad informática y de igual modo garantice una efectiva prestación a los usuarios, donde velen por salvaguardar de los datos de estos.

Ahora bien, el factor principal es el desconocimiento de las herramientas que sirven para evitar o mitigar los efectos de ciberataque, es por ello, que ha de primar el factor educacional frente a la importancia de la seguridad informática, como medio para cumplir efectivamente el derecho constitucional de la protección de los datos personales en todas las esferas sociales, siendo el más apropiado para el desarrollo de este trabajo el sector de las entidades financieras. Es por lo que Suárez (2020), nos dice, que mientras los empleados no cuenten con la formación y conocimiento adecuado, va a ser cada vez más complejo, ya que los ciberdelincuentes tendrán espacios para vulnerar y explotar cualquier dominio, siendo uno de cada cinco empleados una brecha de seguridad (p.10).

Es importante exponer las ventajas que representa la implementación de las técnicas del Big data en las entidades financieras de Colombia:

> VARIEDAD. La última V se refiere a la variedad de diferentes tipos de datos y estructuras, que, en la medida de lo posible, deben tratarse de forma normalizada y armonizarse, para que puedan ser combinados correctamente. Se puede hacer una distinción básica entre los datos estructurados, semiestructurados y no estructurados.
>
> Los datos de cliente maestros son un ejemplo de un formato estructurado e incluyen género, fecha de nacimiento y dirección. Las imágenes, videos y archivos de audio son tipos de datos no estructurados. Los correos electrónicos, por otra parte, se clasifican como semiestructurados porque la información de cabecera contiene datos estructurados, es decir, remitente, destinatario y sujeto, el cuerpo del mensaje no tiene una estructura predefinida. (Jaime, 2017, p. 6)

De igual forma, ante esta situación es detectado por parte de los investigadores cuál es el método que están implementando en la actualidad, un nuevo fraude que se basa en ingeniería social, denominado "CoreBot" un malware que permite personalizar según la víctima y que brinda las características necesarias para cada intrusión, ya que este inyecta un código en el navegador,

captura formularios y roba credenciales, reúne datos personales e información que las instituciones financieras usan como validador y así cometen un fraude, robando identidad, facilitando el fraude. (Asobancaria & OEA, 2019, p. 50).

En un informe realizado por Asobancaria y la OEA, identifican que las empresas no implementan los mecanismos adecuados para su protección y por consiguiente el Banco Bilbao Vizcaya Argentina, a través de sus expertos en ciberseguridad identificaron el eslabón más débil en la protección de datos, que es el ser humano, ya sea el usuario o un empleado de la entidad financiera, aunque las amenazas casi siempre son de terceros, se identifica que cada empleado puede ser un punto de contacto para atacar la organización, ante esto la formación debe ser crucial para frenar este fenómeno de la ciberdelincuencia. (BBVA, 2018, p. 3).

Ante esto muchos usuarios manifiestan temor o desconfianza frente a la proporción de datos que han de brindar especialmente al sector bancario, donde el índice de confianza baja, debido a que: "frente a incidentes de seguridad digital, se han visto comprometida la confidencialidad, integridad o disponibilidad de su información o sus recursos financieros en su banco" (OEA, s.f).

Por último, se ha de resaltar la necesidad que existe en Colombia para que se implementen medidas de protección de datos personales y que estas estén relacionadas con la Inteligencia Artificial (IA), ya que el big data y el uso de las herramientas de la IA, generan riesgos para el titular de los datos. Como la creación de perfiles que pueden resultar iguales o en ocasiones no, robos, extorsiones, suplantación de identidad e inclusive usos para fines políticos ilegales. (Devia, 2019).

III. Las Obligaciones Y Sanciones A Las Que Están Sujetas Las Entidades Financieras.

En Colombia, existen diferentes entidades reguladoras, como las Superintendencias, que según el artículo 66 de la (Ley 489, 1998) son entidades que cumplen funciones de inspección y vigilancia, atribuidas por la ley, consta de diez entidades encargadas de vigilar determinadas actividades económicas en dicho territorio y cada una está definida por un sector en específico.

Las entidades financieras son sujetos de especial control y vigilancia, que es ejercido por la Superintendencia Financiera cuyo objetivo, "es supervisar el sistema financiero colombiano con

el fin de preservar su estabilidad, seguridad y confianza, así como, promover, organizar y desarrollar el mercado de valores colombiano y la protección de los inversionistas, ahorradores y asegurados". (Superintendencia Financiera, s.f, p.1).

En el compendio normativo se ha de determinar la competencia, partirá del artículo 17 de la Ley 1266 de 2008, es aquí donde se establece la competencia, para poder determinar según sea el caso, y de quien se encuentre operando la información, es por ello por lo que, la

> Superintendencia de Industria y Comercio ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera (…) y en los casos en que la fuente, usuario u operador de información sea una entidad vigilada por la Superintendencia Financiera de Colombia, esta ejercerá la vigilancia e impondrá las sanciones correspondientes. (Ley 1266, 2008, p.1)

Ahora bien, la superintendencia financiera ejerce la función de vigilancia en materia de habeas data respecto de una persona natural o jurídica.

> En consecuencia, esta Autoridad ejerce la referida función sobre aquellas instituciones (fuentes y usuarios) que son sus vigiladas en los términos del numeral 2 del artículo 325 del Estatuto Orgánico del Sistema Financiero -EOSF- (Decreto 663 de 1993) y en el numeral 1 del parágrafo 3 del artículo 75 de la Ley 964 de 2005, y la Superintendencia de Industria y Comercio para las demás personas. (Superfinanciera, derecho de petición, 2020, p.2)

De acuerdo con lo anterior tiene la superintendencia financiera la facultad sancionatoria sobre las entidades financieras en materia de habeas data, todo por concepto legal, es decir, el decreto 663 de 1993 en el artículo 335 denominado "procedimientos administrativos aplicable a la superintendencia bancaria "precisamente en el numeral 2 establece:

> Controles por declaración y presunción de veracidad de la información financiera y contable. La información financiera y contable que las entidades vigiladas envíen a la Superintendencia Bancaria en relación con el cumplimiento de las normas que rigen su funcionamiento y el desarrollo de sus operaciones, tales como los informes de encaje, niveles adecuados de patrimonio, margen de solvencia, inversiones obligatorias, máximos o mínimos de inversión, constituyen declaración sobre su cumplimiento. Junto con esta declaración deberán presentarse las explicaciones que a juicio de la entidad se consideren necesarias para el ejercicio de su derecho de defensa si se ha producido una infracción o incumplimiento de tales normas.
>
> Sin perjuicio de lo anterior, la Superintendencia Bancaria podrá en cualquier momento solicitar a las entidades vigiladas que le presenten, dentro del plazo por ella señalado, las informaciones adicionales que estime pertinentes, las cuales constituirán, igualmente, declaración sobre el asunto correspondiente. (Decreto Ley 663,1993, p.1)

Asimismo, el numeral 4 del artículo 335 del decreto en mención indica, dentro de las funciones que ejercen las superintendencias y las atribuciones que le brinda la ley, como este caso en particular, dicho artículo brinda la potestad sancionatoria, facultando para la imposición de sanciones a aquellas entidades que estén sometidas al control y vigilancia de la Superintendencia Bancaria, ahora Superfinanciera. (Decreto Ley 663, 1993, p.1).

Por su parte el estatuto orgánico Financiero mediante artículo 208, especificadamente en el 209 a 211 preceptúa que el Régimen Sancionatorio personal corresponde a Directores, Administradores, Representantes legales, Revisores fiscales u otros funcionarios o empleados, que están sujetos a multa pecuniaria, sanciones, suspensión o inhabilitación por 5 años, remoción de los administradores, clausura de las oficinas, etc. En cuanto al régimen sancionatorio institucional, es propio de las instituciones que son susceptibles de ser supervisadas por la Superintendencia Financiera.

Ahora bien, todo esto analizado desde el punto de vista sancionatorio que le es otorgado a dichas entidades, que pueden interponer medidas administrativas como multas de carácter personal o en su caso a personas jurídicas, como consta en la plataforma de Sanciones en firme que dispone la Superintendencia Financiera conocido como "SIRI"[12], y en el caso de la Superintendencia de Industria y Comercio que también posee dicha facultad, siendo esta la autoridad que vela por la protección de datos, es por ello que, Superindustria multa a CIFIN por incluir sanciones políticas en historial crediticio, es por ello que en su rol de autoridad nacional de protección de datos, impuso una multa por $702.242.400 a la Central de Información Financiera - CIFIN -, por incluir información que no era de carácter financiero o crediticio en el historial de 288.753 colombianos. (Superintendencia de Industria y Comercio, 2020).

Lo anterior, va conforme a la manera en que procede administrativamente, aunque de igual modo, estas entidades pueden ser objeto de sanciones civiles, partiendo de la relación contractual que nace entre el usuario y la entidad, que cuyo objeto es la prestación de un servicio, ante esto nace la Ley 1328 de 2009, que es por la cual se dictan normas en materia financiera o mejor conocida como la protección del consumidor financiero y especialmente en el artículo Séptimo (7), indica cuáles son las obligaciones de las entidades vigiladas y una de ellas es el literal

[12] https://wl.superfinanciera.gov.co/SiriWeb/publico/sancion/rep_sanciones_general.jsf

> b) Entregar el producto o prestar el servicio debidamente, es decir, en las condiciones informadas, ofrecidas o pactadas con el consumidor financiero, y emplear adecuados estándares de seguridad y calidad en el suministro de los mismos. (Ley 1328, 2009)

Este literal indica que es obligación por parte de la entidad financiera de brindar la protección a los servicios que ofrece, establecer todos los mecanismo necesarios para que se cumpla cabalmente lo pactado en el contrato, es decir; el banco tiene por objeto la salvaguarda, la protección del dinero, por ende, es responsabilidad de las entidades financieras la guarda de este, es por ello que estas normas tiene una aplicación preferente, es una norma de destinada al régimen general de las entidades bancarias. Ante esto, las entidades bancarias en el marco constitucional, ha sido definidas las actuaciones bancarias como una actividad de servicio público, lo define la Corte Constitucional en la sentencia SU 157/1999:

> *Pese a que no existe norma que de manera expresa así lo determine, en el derecho Colombiano es claro que la actividad bancaria es un servicio público, pues sus nítidas características así lo determinan. La importancia de la labor que desempeñan para una comunidad económicamente organizada en el sistema de mercado, el interés comunitario que le es implícito, o interés público de la actividad y la necesidad de permanencia, continuidad, regularidad y generalidad de su acción, indican que la actividad bancaria es indispensablemente un servicio público. (Corte Constitucional de Colombia, Sentencia SU 157, 1999)*

De igual forma, en el estatuto del consumidor - la Ley 1480 de 2011, normatividad que regula y establece la eficacia de la prestación de los servicios y cuyas disposiciones especiales, donde se conforma un régimen de carácter especial para una efectiva protección al consumidor en el área bursátil, financiero y de seguros,

> ARTÍCULO 6o. CALIDAD, IDONEIDAD Y SEGURIDAD DE LOS PRODUCTOS. Todo productor debe asegurar la idoneidad y seguridad de los bienes y servicios que ofrezca o ponga en el mercado, así como la calidad ofrecida. (p.4)

> ARTÍCULO 50. Sin perjuicio de las demás obligaciones establecidas en la presente ley, los proveedores y expendedores ubicados en el territorio nacional que ofrezcan productos utilizando medios electrónicos, deberán: f) Adoptar mecanismos de seguridad apropiados y confiables que garanticen la protección de la información personal del consumidor y de la transacción misma. El proveedor será responsable por las fallas en la seguridad de las transacciones realizadas por los medios por él dispuestos, sean propios o ajenos". (Ley 1480, 2011, p. 16)

Conforme a lo anterior, se entiende que, al surgir una relación contractual con las entidades financieras, estas deben de cumplir a cabalidad, todas aquellas obligaciones que nacen producto

de ese negocio, es por ello por lo que, ante cualquier situación que se genere, ellos serán responsables de cualquier afectación o perjuicio que se les pueda ocasionar en el transcurso de la actividad profesional que las entidades financieras desarrollan. En este sentido,

> Toda institución financiera realiza una actividad especializada que requiere de una mayor prudencia, de acuerdo con el conocimiento de su actividad, razón por la cual su conducta debe medirse con base en parámetros más severos que aquellos de los particulares. (Padilla Sánchez & Zafra Sierra, 2017)

Ante esto, el Código Civil colombiano contempla en los artículos 1603, 1604 y el artículo 1546 que habla sobre la responsabilidad civil contractual normas que desde hace 100 años regulan que aquellos profesionales que ejerzan estas actividades económicas, que ante el incumplimiento de las obligaciones y si se ocasionaren perjuicios ha de indemnizar (García, *s.f,* p.28).

De igual modo, la Corte Suprema ya se ha pronunciado en otras sentencias respecto a la responsabilidad civil de las entidades financieras por los daños que sufren los clientes de dichas entidades, es por ello por lo que.

> La Corte Suprema de Justicia, en la Sala de Casación Civil el 11 de marzo de 2010, con ponencia del Dr. Arturo Solarte Rodríguez, indicó.
>
> *"Ha de tenerse en cuenta, además, que ha sido criterio constante de esta Corporación considerar que las instituciones financieras, y particularmente las bancarias, están sujetas a un especial régimen de responsabilidad civil frente a los daños que puedan sufrir los clientes o usuarios de sus servicios, el que ha estado presidido, entre otros, por lineamientos tales como que dichos establecimientos son empresarios profesionales que se consideran expertos en la intermediación financiera; que reciben una especial habilitación del Estado para desarrollar su actividad en virtud de la confianza que se deposita en ellos al conferirles la posibilidad de manejar el ahorro del público, por lo que surgen a su cargo especiales deberes de diligencia; que en las operaciones de captación de recursos ordinariamente celebran contratos de depósito irregular en los que el banco se convierte en titular de los recursos transferidos y asume, por ende, obligaciones de resultado para efectos de su restitución. citado por García, s.f, pp. 38-39)*

Finalmente, se ha de concluir respecto de las obligaciones y sanciones a las que están sujetas dichas entidades, por el vínculo fehaciente que nace de la relación entre la entidad financiera y los usuarios, es por ello por lo que se logra vislumbrar todas las sanciones que puede incurrir dicho sector por el mal manejo de los datos personales, toda vez que desde todos los ámbitos; sea civil, administrativo o penal donde responde el sujeto y no la entidad, se le puede

atribuir una responsabilidad, inclusive la procedencia y utilización de dichos mecanismos, pueden ser utilizados los tres de manera conexa.

Conclusiones

Se estipula que en la Ley Estatutaria 1266 del 2008 y la Ley 1851 de 2012 tienen por objeto la protección constitucional de los datos personales, la primera en carácter especialmente financiero, comercial y crediticio, y la segunda de carácter general, donde los garantes en protección de datos es la Superintendencia Financiera y la Superintendencia de Industria y Comercio (Superindustria).

El cambio más destacado que se generó fue la Ley 1273 de 2009 que modificó el código penal toda vez que creó nuevos tipos penales y el bien jurídico tutelado denominado “De la protección de la información y de los datos”. Y en cuanto a la responsabilidad en materia penal se concluye que no existe un tipo penal que sancione la infracción cometida por una persona jurídica, toda vez que responde es el empleado que realice la conducta dentro de la entidad financiera, será el quien de forma personal asuma la sanción o pena. En materia de delitos informáticos, se denota la imposibilidad de identificar de donde provienen los datos o cómo fue su compilación y recolección, debido a que es una estructura organizada adherida a una red gigantesca, es por lo que no hay manera de atribuir la conducta a sujetos específicos por la dificultad investigativa y probatoria debido al gran automatismo que separa el sujeto del hecho.

Así las cosas, la necesidad actual es la modernización de las leyes preexistentes, donde cuya regulación pueda dar una tipificación adecuada y creen nuevos métodos y protocolos de investigación. Por tanto, es menester implementar medidas de protección de los datos personales que busquen restringir los riesgos que crean con el uso de la inteligencia artificial al titular de los datos personales.

De igual modo, las entidades financieras deben realizar inversión en la implementación de mecanismos de protección frente a las nuevas tecnologías, para estar a la vanguardia como otros países, siendo Suecia, Alemania, Irlanda y Japón quienes ostentan el mayor índice de Ciberseguridad, y por último centrarse en métodos preventivos. Es importante resaltar sobre la capacitación del talento humano, por ser una de las brechas en la seguridad informática del sector bancario, quiere decir, formación en seguridad digital o implementación de hackers éticos, que detectan las fallas y brindan posibles soluciones.

Ante la correcta circulación de los datos se requiere la autorización previa del titular de la información, toda vez que la Circular Externa 018 de 2016, de la Superfinanciera les prohíbe incorporar prácticas y cláusulas abusivas en los contratos realizados con entidades financieras y que no se puede mediante una sola firma, autorizar el total manejo de información personal arguyendo que estos solo pueden ser destinados de acuerdo al negocio jurídico realizado, basando en el principio de finalidad y necesidad expresados por la Corte Constitucional.

La Superintendencia Financiera de Colombia tiene la facultad para vigilar y sancionar de acuerdo con la naturaleza a la fuente o usuario, ya que así lo establece el decreto 633 de 1993 en su artículo 325 numeral 2 denominado el Estatuto orgánico del Sistema Financiero EOSF. Donde las personas jurídicas, suelen ser las primeras responsables, dado que están sujetas a la vigilancia y sanción de las superintendencias, cuya competencia se define según la naturaleza. Por tanto, las entidades financieras son sancionadas y se les imponen elevadas multas. Por último, mediante artículo 208, especificadamente en el 209 a 211 preceptúa que el Régimen Sancionatorio personal corresponde a Directores, Administradores, Representantes legales, Revisores fiscales u otros funcionarios o empleados, los cuales están sujetos a multas, suspensiones y amonestaciones.

Referencias

Aldania, R. C. (2004). *Aproximaciones para una historia de Internet. 12*(1). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S102494352004000100005&lng=es&nrm=iso>1

Angarita, N. R. (2010). *¿Tiene Colombia Un Nivel Adecuado De Protección De Datos Personales A La Luz Del Estándar Europeo? (ISSN 1692-8156), 16*. Revista Colombiana de Derecho Internacional. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S169281562010000100015&lng=en&nrm=iso&tlng=es >2

Aristizábal, S. R. (2019). *Revisión de literatura de macrodatos (Big data)*. 20. Pereira, Colombia: Universidad EAFIT, 20. https://repository.eafit.edu.co/handle/10784/14300 >3

Asamblea General de Las Naciones Unidas. (10 de Diciembre de 1948). *Declaración Universal de los Derechos Humanos*. *(Resolución 217 A (III* https://www.un.org/es/universal-declaration-human-rights/ > 4

Asobancaria [CSIRT]. (19 de Abril de 2019). La apuesta de la banca por la ciberseguridad: CSIRT financiero.https://www.csirtasobancaria.com/saladeprensa/laapuestadelabancaporlaciberseguridad-csirtfinanciero >5

Asobancaria. (6 de Agosto de 2018). Semana Económica 2018. *Retos de Colombia en ciberseguridad a propósito de la adhesión al "Convenio de Budapest", Edición 1148*. https://www.asobancaria.com/wp-content/uploads/1148.pdf >6

Asobancaria. (30 de Septiembre de 2019). Semana Económica 2019. *Gestión de riesgos en el marco de la era digital, 1204*. https://www.asobancaria.com/wp-content/uploads/semana-economica-edicion-1204.pdf >7

Asobancaria, Organización de los Estados Americanos (OEA). (Octubre de 2019). *Desafíos del riesgo cibernético en el sector financiero para Colombia y américa latina.* https://www.asobancaria.com/wp-content/uploads/20191010-asobancaria-OEA_min.pdf >8

Banco Bilbao Vizcaya Argentina (BBVA). (26 de Abril de 2018). *La ciberdelincuencia, una amenaza para la banca de América Latina*. *Innovación*. https://www.bbva.com/es/ciberdelincuencia-amenaza-banca-america-latina/ >9

Banco Bilbao Vizcaya Argentina [BBVA]. (18 de Agosto de 2017). Innovación digital en servicios financieros: retos para los reguladores. *Beneficios y riesgos de la transformación de los servicios financieros*, 8. (S. F. Lis, Ed.) https://www.bbvaresearch.com/publicaciones/innovacion-digital-en-servicios-financieros-retos-para-los-reguladores/ >10

BBC Mundo. (16 de Octubre de 2016). Qué es la cuarta revolución industrial (y por qué debería preocuparnos). (V. Perasso, Ed.) https://www.bbc.com/mundo/noticias-37631834 >11

Bravo, R. H. (2011). Cloud Computing Y Seguridad Despejando Nubes Para Proteger Los Datos Personales. *Revista de derecho y ciencias penales: Ciencias Sociales y Políticas*, *17*(ISSN 0718-302X), 43-58. https://dialnet.unirioja.es/servlet/articulo?codigo=4200372 >12

Buitrago, E. R. (20 de Enero de 2015). *La práctica de delitos informáticos en Colombia.* Bogotá, Colombia: Universidad Militar Nueva Granada. http://hdl.handle.net/10654/13452 > 13

Carrasco, D. O. (2009). *Cómo escribir artículos de revisión*. *15(1)*. La paz, Bolivia: Revista Médica La Paz. http://www.scielo.org.bo/scielo.php?pid=S1726-89582009000100010&script=sci_arttext >14

Castillo, Z. N. (2017). *Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia*. Chiquinquirá, Colombia: Universidad Nacional Abierta Y A Distancia [UNAD]. https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1&isAllowed=y > 15

Congreso de Colombia. (2 de Abril de 1993). Decreto Ley 663 De 1993. *Estatuto Orgánico Del Sistema Financiero*.http://secretariasenado.gov.co/senado/basedoc/estatuto_organico_sistema_financiero.html>16

Congreso de Colombia. (30 de Diciembre de 1998). Ley 489 De 1998. *Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189.* http://www.secretariasenado.gov.co/senado/basedoc/ley_0489_1998.html#1>17

Congreso de Colombia. (24 de Julio de 2000). Ley 599 De 2000. *Por la cual se expide el Código Penal*. http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html > 18

Congreso de Colombia. (31 de Diciembre de 2008). Ley Estatutaria 1266 De 2008. *Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dicta*. http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html > 19

Congreso de Colombia. (05 de Enero de 2009). Ley 1273 De 2009. *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comu*. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html >20

Congreso de Colombia. (15 de Julio de 2009). Ley 1328 de 2009. *Por la cual se dictan normas en materia financiera, de seguros, del mercado de valores y otras disposiciones*. http://www.secretariasenado.gov.co/senado/basedoc/ley_1328_2009.html >21

Congreso de Colombia. (12 de Octubre de 2011). Ley 1480 del 2011. *"Por Medio De La Cual Se Expide El Estatuto Del Consumidor Y Se Dictan Otras Disposiciones"*, 1-33. https://www.sic.gov.co/recursos_user/documentos/normatividad/Leyes/2011/Ley_1480_Estatuto_Consumidor.pdf>22

Congreso de Colombia. (18 de Octubre de 2012). Ley Estatutaria 1851 De 2012. *Por la cual se dictan disposiciones generales para la protección de datos personales*. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html >23

Constitución Política de Colombia. (1991). Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html >24

Corte Constitucional de Colombia. (10 de Marzo de 1999). Sentencia SU 157/ 1999 Referencia: Expedientes T-153.327 y T-152.413 (acumulados). *[M.P Dr. ALEJANDRO MARTÍNEZ CABALLERO]*. https://www.corteconstitucional.gov.co/relatoria/1999/SU157-99.htm >25

Corte Constitucional de Colombia. (16 de Octubre de 2008). Sentencia C-1011/08 Referencia: expediente PE-029. *[M. P Dr. JAIME CÓRDOBA TRIVIÑO]*. https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm >26

Corte Constitucional de Colombia. (27 de Enero de 2014). Sentencia T-020/2014. *Referencia: Expediente T-4.033.635 - [M.P LUIS GUILLERMO GUERRERO PÉREZ]*.https://www.corteconstitucional.gov.co/relatoria/2014/T02014.htm#:~:text=El%20principio%20de%20finalidad%20supone,fin%20que%20abarca%20su%20manejo. >27

Corte Suprema de Justicia, Sala de Casación Penal. (11 de Febrero de 2015) Sentencia SP1245-42724. [MP EYDER PATIÑO CABRERA]. https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf > 28

COUNCIL OF EUROPE. (23 de Noviembre de 2001). Convenio Sobre La Ciberdelincuencia. *(Serie de Tratados Europeos N°185)*, 2. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf > 29

Departamento Nacional de Planeación. (11 de Abril de 2016). Consejo Nacional de Política Económica y Social. *Documento Conpes 3854*, 26. https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNPConpesPol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y >30

Devia, A. M. (Enero- Junio de 2019). La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? *5-23(27)*. Revista la Propiedad Inmaterial. https://doi.org/10.18601/16571959.n27.01 >31

García, J. D. (s.f). *Dinero, Tecnología Y Prueba Indiciaria Una Mirada A La Responsabilidad Civil De Los Bancos En El Fraude Electrónico*. http://felaban.s3.amazonaws.com/colade/monografias/2014/1%20Colombia%20%20C%20Senior%20%20Monografia%20%20CONFERENCIA%20DINERO%20TECNOLOGIA%20Y%20PRUEBA%20INDICIARIA%20777.pdf>32

Institute of International Finance [IIF]. (13 de October de 2017). *Digital transformation and cybersecurity are top concerns of CROs*. https://www.iif.com/Press/View/ID/261/Digital-transformation-and-cybersecurity-are-top-concerns-of-CROs>33

JAIME, C. A. (2017). *Usos del Big data en la administración de las relaciones con el cliente en las empresas financieras de Colombia.* 6. Universidad Libre de Colombia. https://repository.unilibre.edu.co/bitstream/handle/10901/11211/USOS%20DE%20DEL%20BIG%20DATA%20EN%20LA%20ADMINISTRACI%C3%93N%20DE%20LAS%20RELACIONES%20CON%20EL%20CLIENTE%20EN%20LAS%20EMPRESAS%20FINANCIERAS%20DE%20COLOMBIA.pdf?sequence=1 >34

MARTÍNEZ, M. O. (2018). *La Responsabilidad Penal De Las Personas Jurídicas En Colombia Y El Compliance*. 9. Universidad Libre de Colombia. https://repository.unilibre.edu.co/bitstream/handle/10901/17996/RESPONSABILIDAD%20PENAL%20DE%20LAS%20PERSONAS%20JURIDICAS.pdf?sequence=1&isAllowed=y>35

Ministerio de Tecnologías de la Información y Comunicación [MinTIC]. (Marzo de 2014). Sistemas de Investigación, Desarrollo e Innovación. *Agenda Estratégica de Innovación- Nodo Ciberseguridad*, https://www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdf >36

Kaiser, B. (2019). La Dictadura de los Datos. *La verdadera historia dentro de Cambridge Analytica y de cómo el Big Data, Trump y Facebook rompieron la democracia y cómo puede volver a pasar (I.S.B.N.: 978-84-9139-427-3)*, 16. (C. R. Malavé, Trad.). HarperCollins Ibérica S.A. https://books.google.com.co/books/about/La_dictadura_de_los_datos.html?id=3D68DwAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=snippet&q=En%20la%20era%20digital%2C%20los%20datos%20son%20el%20nuevo%20petr%C3%B3leo&f=false >37

Organización de Estados Americanos (OEA), (s.f). *Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.* 13. Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo. https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf >38

Organización para la Cooperación y el Desarrollo Económicos [OECD]; Banco Interamericano de Desarrollo [BID]. (Diciembre de 2016). *Políticas de Banda Ancha para América Latina y el Caribe: Un Manual para la Economía Digital. (ISBN 978-92-64-26535-6)*. París. https://publications.iadb.org/publications/spanish/document/Pol%C3%ADticas-de-banda-ancha-para-Am%C3%A9rica-Latina-y-el-Caribe-Un-manual-para-la-econom%C3%ADa-digital.pdf >39

Fiscalía General de la Nación. (14 de Septiembre de 2018). Capturadas 121 personas por delitos informáticos. *Jornada nacional contra la cibercriminalidad*. https://www.fiscalia.gov.co/colombia/seccionales/capturadas-121-personas-por-delitos-informaticos/ > 40

Padilla Sánchez, J. A., & Zafra Sierra, M. (Enero-Junio de 2017). Responsabilidad de los establecimientos bancarios por el pago de cheques falsos o alterados en Colombia. (U. E. Colombia, Ed.) *Revista de Derecho Privado* (32), 383-420. https://doi.org/10.18601/01234366.n32.13. >41

Policía Nacional de Colombia. (29 de Octubre de 2019). Informe de Tendencias del Cibercrimen en Colombia. *Tendencias Cibercrimen Colombia 2019-2020, Primera Edición*. https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf > 42

Prieto, A., & Martínez, M. (2004). *Sistemas de información en las organizaciones: Una alternativa para mejorar la productividad. Revista de Ciencias Sociales*, *2*(ISSN 1315-9518), 322-337. https://www.redalyc.org/articulo.oa?id=28010209 > 43

Suárez, J. L. (Agosto de 2020). *Importancia de la Seguridad Informática y Ciberseguridad en el Mundo Actual*. 1-12. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/8668 >44

Superintendencia de Industria Y Comercio. (20 de Abril de 2020). Superindustria sanciona a Scotiabank Colpatria por incumplir ley de protección de datos. https://www.sic.gov.co/slider/superindustria-sanciona-scotiabank-colpatria-por-incumplir-ley-de-protecci%C3%B3n-de-datos >44

Superintendencia de Industria Y Comercio. (*s.f.a*). *Protección de Datos Personales*. Bogotá, Colombia. Recuperado el 24 de 08 de 2020, de https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales > 45

Superintendencia de Industria y Comercio. (*s.f.b). Protección de los Datos Personales: Aspectos Prácticos Sobre El Habeas Data*. https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Aspectos_Derecho_de_Habeas_Data.pdf > 46

Superintendencia Financiera de Colombia. (26 de Mayo de 2016). Circular Externa 018 de 2016. https://xperta.legis.co/visor/temp_legcol_5d61dcb4-ed52-4e83-8200-dc1de44b2dc6 >47

Superintendencia Financiera. (2020). Trámite:115-*Consultas Generales Y Administrativas*. *(Radicación:2020198778-003-000)*, 1-3. Remitente: 70310-70310-GRUPO DE DOCTRINA UNO.https://www.superfinanciera.gov.co/formulesuqueja/faces/consulta/consultaExterna.xhtml> 48

Superintendencia Financiera. (s.f). Acerca de la SFC-Propósito Superior de la Superintendencia Financiera de Colombia. *Naturaleza jurídica y objeto*. https://www.superfinanciera.gov.co/jsp/60607>49

Universidad Sergio Arboleda. (s.f). En la Sergio. *CUARTA REVOLUCIÓN INDUSTRIAL: ¿Qué Es El Mundo 4.0?* https://www.usergioarboleda.edu.co/noticias/cuarta-revolucion-industrial-que-es-el-mundo-4-0/ >50