Breve análisis sobre Big Data y la protección al usuario del Sistema Bancario Venezolano

Kimberly K. González Rojas[*]
Génesis D. Gutiérrez Rosales[**]
Daniela Linares Gatti[***]

RVDM, nro. 12, 2024, pp. 581-611

Resumen: El surgimiento de la sociedad de la información y el empleo de la Big Data ha permitido que las instituciones del sector bancario accedan a cada vez mayores volúmenes de datos personales sobre sus clientes y usuarios, lo que permite tomar decisiones más efectivas que incrementen la calidad del servicio prestado y de los productos ofrecidos. Ante esto, la legislación debe proporcionar al individuo la debida protección a sus derechos fundamentales, dentro de un compás de apego a los principios que orientan un correcto tratamiento de datos y reduciendo los riesgos por un eventual procesamiento indebido.

Palabras clave: Big data, Sistema Bancario, Protección de Datos, Habeas data.

Brief analysis of Big Data and user protection of the Venezuelan Banking System

Abstract: *The emergence of the information society and the use of Big Data has allowed institutions in the banking sector to access increasing volumes of personal data about their clients and users, allowing them to make more effective decisions that increase the quality of the service provided and products offered. Given this, legislation must provide the individual with due protection of their fundamental rights, within a compass of adherence to the principles that guide correct data processing and reducing the risks of possible improper processing.*

Keywords: *Big Data, Data Protection, Financial System, Habeas Data.*

Recibido: 17/5/2024
Aprobado: 31/5/2024

[*] Abogada, Universidad Central de Venezuela. Año 2012. Cursante de la Especialización en Derecho Mercantil en la misma Casa de Estudios.

[**] Abogada, Universidad Central de Venezuela. Año 2018. Cursante de la Especialización en Derecho Mercantil en la misma Casa de Estudios.

[***] Abogada, Universidad Central de Venezuela. Año 2018. Licenciada en Estudios Internacionales, UCV 2022.Cursante de la Especialización en Derecho Mercantil, de la Especialización en Derecho de la Navegación y Comercio Exterior y de la Maestría en Derecho Internacional Privado y Comparado en la misma Casa de Estudios.

Breve análisis sobre Big Data y la protección al usuario del Sistema Bancario Venezolano

Kimberly K. González Rojas[*]
Génesis D. Gutiérrez Rosales[**]
Daniela Linares Gatti[***]

RVDM, nro. 12, 2024, pp. 581-611

SUMARIO:

INTRODUCCIÓN

En la sociedad actual la información resulta una pieza clave, lo que convierte a la recolección, procesamiento, almacenamiento y tratamiento de los datos personales en un tema de gran relevancia. El incremento del uso de la tecnología, el avance del Internet de las Cosas o *IoT* y la penetración cada vez mayor del comercio electrónico y las redes sociales, aparejadas del uso de la inteligencia artificial, han ubicado al sistema bancario en una situación estratégica en cuanto a la captación de información sobre sus clientes y relacionados, respecto a sus transacciones, patrones de consumo e historial crediticio.

---

[*] Abogada, Universidad Central de Venezuela. Año 2012. Cursante de la Especialización en Derecho Mercantil en la misma Casa de Estudios.

[**] Abogada, Universidad Central de Venezuela. Año 2018. Cursante de la Especialización en Derecho Mercantil en la misma Casa de Estudios.

[***] Abogada, Universidad Central de Venezuela. Año 2018. Licenciada en Estudios Internacionales, UCV 2022.Cursante de la Especialización en Derecho Mercantil, de la Especialización en Derecho de la Navegación y Comercio Exterior y de la Maestría en Derecho Internacional Privado y Comparado en la misma Casa de Estudios.

Por su función de intermediación en el sistema financiero, las instituciones bancarias reciben de sus clientes una gran cantidad de información personalísima, que con la entrada en funcionamiento de la tecnología a gran escala, forma parte de grandes bases de datos o sistemas de información que reportan a la banca numerosas utilidades al permitirles conocer de manera más precisa las necesidades e intereses de sus clientes o potenciales clientes, sus patrones de consumo, los productos financieros acordes con su capacidad económica e inclusive la necesidad de una sucursal o agencia bancaria en una determinada localidad.

Para obtener utilidad de toda esta información, conocida como Big Data, los bancos recurren al procesamiento de datos con mecanismos que cada vez exigen mayor eficiencia, exactitud y celeridad, lo que en modo alguno debe resultar perjudicial para el usuario, quien es el único propietario y titular de la información contenida en dichos sistemas, los cuales deben contar con las garantías adecuadas que le permitan ejercer sus derechos de contraloría sobre tales datos que deben ser verosímiles, exactos, completos y vigentes, contando en caso contrario con las vías legales para ejercer oportunamente sus pretensiones, a fin de que la información errónea sea rectificada e incluso eliminada a la mayor brevedad posible.

En Venezuela, la Constitución de 1999 consagra en su articulado la protección de los derechos a la información, a la intimidad y a la autodeterminación informativa o habeas data. No obstante, hasta la fecha de elaboración de esta investigación el ordenamiento jurídico venezolano no cuenta con una ley especial en materia de protección de datos. Sin embargo, tímidamente han surgido ciertas disposiciones legales aisladas que hacen una mención tangencial a la materia, pero sigue existiendo una mora del legislador venezolano hacia el desarrollo de la protección de este derecho fundamental, como ha sido el caso de los países europeos y ciertos países latinoamericanos.

En el presente trabajo, abordaremos la definición de la Big Data, su importancia actual y el futuro de su utilización por las instituciones del sector bancario. Asimismo, consideraremos la protección de datos, el alcance de los derechos de los particulares en esta materia, los principios que rigen el tratamiento de datos, así como los riesgos a los cuales se encuentran sometidos los datos personales suministrados a la banca, haciendo una especial referencia al caso venezolano, aportando finalmente nuestras conclusiones sobre el tema planteado.

1. Big data. Su importancia y utilización por las instituciones del sector bancario

Desde el nacimiento de la *World Wide Web* (www) ha aumentado significativamente el nivel de información al que estamos expuestos, ya que se define como una red de datos interconectada a nivel mundial. Hoy en día no puede imaginarse el desarrollo de distintos procesos sin la asistencia de esta herramienta, pero es difícil calcular los niveles de información que ésta es capaz de generar y el miedo inicial es no saber cómo procesar tanta abundancia de datos.

Actualmente, la información es poder para las grandes empresas y la banca no escapa de esta realidad. Con base en esta premisa, es que se genera la carrera por la obtención de la mayor cantidad de información de calidad posible, por lo que hoy en día todos buscan la Big Data[1].

La Big Data se define como el conjunto de datos cuyo tamaño, complejidad y crecimiento acelerado dificultan su análisis a través de medios tradicionales, tales como una base de datos simple, estadísticas convencionales, métricas simples, entre otros. Debido al contenido tan grande y variado que maneja, se ha convertido en una nueva fuente de valor para las empresas, ya que el análisis certero de la misma es lo que permite su utilización final.

Una forma sencilla de saber si estamos en presencia de Big Data, es por el peso de los datos. Muchos establecen que van desde 30-50 Terabytes a varios Petabytes. Muchas veces son datos no estructurados o clasificados en conjuntos de datos, lo cual dificulta en un primer momento su análisis. Depende mucho de los procesos de digitalización que lleven a cabo las empresas, los cuales son algo corriente en los tiempos modernos, lo que ha llevado a buscar apoyo en sistemas más complejos, como aquellos que trabajan con datos biométricos o inteligencia artificial.

La mayoría de dispositivos que se utilizan en la cotidianidad generan data: laptops, celulares, aplicaciones, correos electrónicos, uso de tarjetas de crédito o débito, entre otras, que se generan en todo momento y lugar. Con base en esto, lo más importante es la capacidad de procesamiento de la misma a la mayor velocidad posible, por lo que se han desarrollado programas como CRM (*Customer Relationship Management*) o ERP (*Enterprise Resource Planning*)[2] para poder desglosar la misma y aprovecharla, reduciendo costos de trabajar con programas más tradicionales, que requieren mucho más tiempo y energía para funcionar.

---

[1] S/A. Big Data: "¿En qué consiste? Su importancia, desafíos y gobernabilidad". Power Data, 2023 *Power Data.* 2023. https://www.powerdata.es/big-data. (último acceso: 04 de diciembre de 2023).

[2] S/A. Big Data: "¿En qué consiste? Su importancia, desafíos y gobernabilidad". Power Data, 2023 *Power Data.* 2023. https://www.powerdata.es/big-data. (último acceso: 04 de diciembre de 2023).

Estos programas tienen una base preestablecida por los usuarios de cada módulo del mismo, con el fin de adaptarlos a sus necesidades y obtener la data y métricas necesarias para mejorar en sus funciones y gestionar la prevención de riesgos, aumentando la efectividad a la hora de dar respuesta. Se busca que la Big Data sea variada y veloz, pero también veraz y de valor, para poder analizarla adecuadamente.

La importancia de la Big Data hoy en día radica en la posibilidad de procesar dichos datos a gran velocidad para detectar necesidades, intereses y oportunidades con la información que dan los usuarios en relación a preferencias, incidencias, calidad de los productos y servicios, entre otras variables diversas. La idea principal es la anticipación a la resolución de posibles incidencias, métricas de productos actuales y futuros, así como el manejo de control de calidad. También puede ejercer una función de prevención de incidencias al verse reportadas como una anomalía, lo cual permite su rápida reversión y prevención en casos futuros.

A través de las redes sociales y aplicaciones móviles, también se permite una mejor publicidad con reducción de costes y enfocada directamente a los clientes que ya se tienen, aumentando las posibilidades de recompras de productos o servicios, contratación de nuevos elementos en los catálogos de las empresas y una sensación de inmediatez con el usuario, aumentando de este modo sus niveles de satisfacción.

Para la banca, el Siglo XXI ha sido un período de muchos cambios en poco tiempo, lo cual la ha obligado a adaptarse si no quiere perder relevancia, como se ve en los procesos de digitalización, mejores medios de pago, adaptación a las criptomonedas bajo sus propios términos (CBDC: Central Bank Digital Currency), entre otros. Parte de esa adaptación se encuentra en el uso y aprovechamiento de la Big Data, ya que se permite procesar las solicitudes de los usuarios nuevos y existentes a una mayor velocidad para responder de forma satisfactoria a las mismas, al tiempo que se mantienen dentro de la vanguardia tecnológica.

El usuario es aquella persona que utiliza un servicio, esperando que el mismo sea de calidad y responda a sus necesidades. Se diferencia de un consumidor por el tipo de bien que solicita (producto vs servicio), por su frecuencia de uso y porque no suele valorar los mismos elementos de un servicio que de un producto. El usuario no tendría una posesión del servicio (lo que si pasa al adquirir un producto), sino que disfruta del mismo haciendo un pago o efectuando una suscripción determinada.

En Venezuela, la protección al consumidor y al usuario está desarrollada de una manera bastante limitada[3] por la Ley Orgánica Precios Justos de 2015[4], la cual apenas establece en su artículo 7°, numeral 9°, el derecho de las personas a la promoción y protección jurídica de sus derechos e intereses económicos y sociales en las transacciones realizadas, por cualquier medio o tecnología, lo cual deja un vacío en cuanto a la defensa del usuario en relación a la protección de sus datos personales, a diferencia de otras legislaciones que consagran un espectro de protección mucho más específico, tal como se verá más adelante.

Cabe recordar que la Big Data requiere de una arquitectura propia y de su auditoría interna de forma periódica, con el fin de filtrar información y poder usarla de una manera más efectiva. La velocidad de cambio en la información implica que la misma puede perder relevancia rápidamente, por lo que un exceso de data no actualizada se vuelve inútil para la banca y para todo aquél que la necesite.

Una ventaja de la banca es que la data que requiere es mucho más específica que en los casos de otras industrias (comida, redes sociales, vestido), por lo que la segmentación es más directa y sencilla. Sin embargo, su dificultad radica en el número de usuarios que tienen. Para el 2022, el Banco de Venezuela registró 2.292 millones de usuarios bancarizados por ellos, representando el 65% de usuarios de todo el país[5], los cuales tienen necesidades similares que permiten determinar qué debe hacer la banca para satisfacer las mismas.

Sin embargo, un aspecto negativo es la sobreinformación. Todo se puede digitalizar y generar contenido que puede o no ser relevante y no siempre se tiene la capacidad de filtrarlo, por lo que noticias falsas (*fake news*), el contenido *spam* y la información falsa pueden afectar directamente la calidad de la base de datos construida con Big Data. A menor calidad, menor eficiencia de la misma y más espacio ocupado sin aprovecharlo en realidad dentro de las bases de datos.

Esto se materializa al observar las fuentes de la Big Data: datos móviles e internet, el internet de las cosas, datos sectoriales y datos experimentales. Cabe destacar que solo el 20% de esta información se considera verdaderamente estructurada, por lo que parte del trabajo de la Big Data es filtrar la información y clasificar la más relevante para el usuario o el interesado, mientras clasifica, ordena y analiza la información restante para buscar el mejor uso de la misma.

---

3 *Vid*. Chacón, Nayibe. «Reseña histórica de la protección al consumidor y usuario en Venezuela: Mucho más que "precios justos".» *Revista Venezolana de Legislación y Jurisprudencia N° 9*, 2017: 141-165.

4 *Gaceta Oficial de la República Bolivariana de Venezuela* N° 6202 extraordinario, del 08 de noviembre de 2015; reimpresa por error material en la *Gaceta Oficial* N° 40787, del 12 de noviembre de 2015.

5 Banco de Venezuela. *Informe Primer Semestre 2022.* Caracas: Banco de Venezuela, 2022 https://www.bancodevenezuela.com/files/informesgestion/Memoria%20(informe%20Junta%20directiva)I%20Semestre%202022.pdf.

La información estructurada se define como aquella que puede usarse en su forma original al transmitir la información necesaria, mientras que los datos no estructurados se refieren a aquella información no organizada que requiere un mayor nivel de procesamiento para poder aprovecharla, ya que debe clasificarse y organizarse según los parámetros del sistema utilizado en el momento[6].

El sistema de almacenamiento de datos más usado y básico es el de tablas de relacionamiento, donde se organizan los datos de forma estructurada y se conectan por relaciones entre los mismos, dándole un carácter único a cada tabla, pero no es el único sistema que se utiliza hoy en día.

Adicionalmente, siempre se tienen dudas de qué eliminar de la base de datos, lo cual incide en el almacenamiento del sistema a utilizar y cómo puede manejarse el mismo de una manera efectiva. Se trabaja con recursos como la nube y la conservación de datos en la web, lo cual puede causar problemas al momento de enfrentar un robo de datos por la fragilidad de su seguridad de almacenamiento.

Otro elemento a tomar en consideración es la potencial volatilidad de los datos. En el mundo de las redes sociales, las tendencias cambian diariamente, por lo que el procesamiento de la información debe ser lo más rápido y efectivo posible. En el mundo de la banca la data es más estable, pero su volatilidad puede verse condicionada a algún anuncio a futuro o alguna falla en el sistema que lesione la confianza de los usuarios en el mismo.

Si bien en la banca la volatilidad es considerablemente menor, en casos excepcionales como en los cambios de valor de la moneda, anuncios gubernamentales, cambios geopolíticos o decisiones económicas se afecta el comportamiento rutinario de los usuarios en mayor o menor medida en contra del sistema bancario tradicional, por lo que es importante medir estas variables para poder prevenir su impacto y amortiguarlo en la medida de lo posible. En caso de no poder hacerlo o de tener un sistema deficiente, se puede esperar una caída del sistema que lesione la credibilidad y reputación de dicha institución bancaria entre sus usuarios.

La obtención de datos también puede considerarse un problema a pesar de ser una función básica para la operatividad de la Big Data, ya que hay datos que para su obtención requieren la autorización del usuario, mientras que otros se obtienen de forma discreta y sin consentimiento del mismo, lo cual muchas veces puede facilitar la comisión de distintos delitos aprovechando la data centralizada.

---

[6] Cueto, Marta. «Big Data en la banca y sus implicaciones para el futuro.» *Trabajo de Grado. Universidad Pontificia Comillas.* Madrid, 2019. P.6.

El almacenamiento también puede convertirse en una dificultad a largo plazo si no se previene desde el inicio. Igual a un celular que se va quedando sin memoria y genera problemas, puede pasar lo mismo con los sistemas de Big Data, por lo que es importante considerar fuentes de respaldo alternas, almacenamiento en la nube o incluso la eliminación periódica de los datos obsoletos o que ya no se consideren necesarios en un determinado periodo. Lo ideal siempre es tener un sistema que pueda almacenar datos de manera ilimitada, pero ello puede implicar un aumento significativo de costos.

Adicionalmente, no puede soslayarse que la banca trabaja con los denominados datos sensibles, ya que el criterio actual establece que toda la información bancaria de los usuarios (datos personales y operaciones activas o pasivas) deben ser resguardados por los sistemas y estructuras bancarias, ya que su mal uso o difusión pueden afectar negativamente el patrimonio de los clientes, violando de igual modo su derecho a la privacidad.

1.1. Futuro de la Big Data en la banca

Debido al aumento significativo de usuarios y número de transacciones entre ellos, la Big data se consolidará como una herramienta clave para la banca, por lo que se requerirá de su adaptación paulatina a la misma. Los productos tales como el pago móvil, billeteras en divisas, tarjetas de crédito prepagadas y la posibilidad de optar a préstamos son resultado de un análisis certero de esta información con el fin de satisfacer las necesidades de los usuarios.

Adicionalmente, por medio de estas aplicaciones se permite la actualización de los consumos, dirección e ingresos de los usuarios, redirigiendo estrategias de marketing y promoción de productos con el fin de captar *leads* y expandirse en el sector. Sin embargo, no se puede dejar de lado la importancia de la seguridad de los datos y del uso adecuado que se le da a los mismos, ya que usar los mismos para ir más allá de lo acordado no solo puede generar incomodidad en los usuarios, sino el riesgo del robo de datos y una sensación de vulnerabilidad muy difícil de superar.

A medida que la digitalización avance y disminuya el uso de medios físicos de pago, la Big data se mantendrá en constante actualización, por los nuevos movimientos y transacciones que puedan hacer los usuarios a través de los dispositivos móviles y *wallets* digitales, ya que pueden trabajar incluso con tecnología *contactless*, que implica la misma transferencia de data pero por medios electrónicos.

Debido a estas condiciones, también es necesario que el personal bancario reciba los cursos y capacitaciones necesarias para manejar los sistemas de procesamiento de la Big Data que puedan utilizar, ya que deben adaptarse a lo que la banca requiera. Un

ejemplo de ello es que para adaptar el Zoho CRM[7] a una empresa, puede tomar de un mes, a mes y medio, dependiendo de las especificaciones que necesite cada departamento, el volumen de datos a manejar, manejo de incidencias, solicitudes especiales, etc. Cabe recordar que es el sistema el que debe adaptarse al cliente, para que el mismo pueda hacer frente a las necesidades de sus usuarios.

2. Protección de datos. Derechos del titular de la información

Gracias al crecimiento de la banca online y la implementación de la banca móvil, los entes bancarios recogen datos de muchas fuentes en tiempo real, tales como las transacciones de negocios o información recibida a través de las redes sociales para almacenarla, procesarla y darle una posterior utilización que se traduce en mayor transparencia, descubrimiento de necesidades concretas de sus clientes, mejor rendimiento y segmentación de poblaciones para ofrecer servicios diferenciados, de acuerdo a las necesidades de cada grupo.

Datos sobre cada usuario del sistema financiero se recogen a diario a través de operaciones cotidianas que se realizan de manera frecuente al utilizar una tarjeta de crédito, al completar una encuesta en el portal web de la institución bancaria de confianza, al hacer pagos durante un viaje vacacional o realizar el envío de un correo electrónico, además de la gran información que proporcionan las personas mediante la huella digital que deja el uso de diferentes navegadores y las redes sociales.

Mientras que algunos de estos datos requieren de la autorización del titular para ser utilizados o incluso recolectados por terceros, otro tipo de datos pueden tomarse sin que su titular esté en conocimiento de ello. Sin necesidad de profundizar demasiado, la banca conoce datos demográficos como el género, edad y nivel de ingresos económicos de sus clientes; pero más allá de ello, posee una ventaja competitiva al obtener datos sobre las preferencias de cada consumidor, los productos que le atraen o el tipo de plataforma que prefiere para efectuar sus compras, lo que con el respectivo análisis, proporciona información sobre los gustos y preferencias del consumidor, aportando una mejora en sus modelos de negocio, productos y servicios lo que en definitiva, le genera importantes beneficios.

Señala oportunamente Aristeo García González:

> Cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida que afecta potencialmente incluso a los aspectos más sensibles de su vida privada, aquellos que en épocas anteriores quedaban fuera de todo

[7] Software para sistemas de ventas en línea que permite gestionar las ventas, el marketing y el soporte en una sola plataforma de CRM (*Customer Relationship Management*).

> control, por su variedad y multiplicidad y que hoy, además de tomar conciencia de ello, comienzan a exigir un reconocimiento sobre el uso y control de sus datos.[8]

A su vez, el artículo 4° del Reglamento UE 2016/679[9] en materia de protección de datos personales, aporta las siguientes definiciones:

> Se entiende por datos personales toda información sobre una persona física identificada o identificable y («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Prosigue Aristeo García González, citando a Benda: "el peligro para la privacidad del individuo no radica en que se acumule información sobre él, sino, más bien en que se pierda la capacidad de disposición sobre ella y respecto a quién y con qué objeto se transmite."[10]

De acuerdo a los Estándares de Protección de Datos Personales publicados por la Red Iberoamericana de Protección de Datos, el tratamiento es:

> Cualquier operación o conjunto de operaciones efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recolección, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.[11]

Como acertadamente destaca Aponte[12], citando el Anuario de Derecho de las Tecnologías de la Información y las Comunicaciones, la protección de datos personales se puede definir como:

---

8 García, Aristeo. «La protección de datos personales: derecho fundamental del siglo XXI un estudio comparado.» *Boletín Mexicano de Derecho Comparado*, 2007: 743-778. P.752.

9 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

10 García, Aristeo. *Op. Cit*. P. 763.

11 Red Iberoamericana de Protección de Datos. «Estándares de Protección de Datos Personales.» 2017. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

12 Aponte, Emercio. «La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano.» *Revista de Derecho Privado. Universidad Externado de Colombia*, 2007. P.110. En cuanto a este tema, el autor acoge esta definición aceptando como únicos sujetos de protección a las personas naturales. No obstante, hace referencia al Anteproyecto de Ley de Protección de Datos y Habeas Data para Venezuela que extendía la misma a los datos pertenecientes a las personas jurídicas incorporales, al igual que lo hace la legislación vigente en países como Argentina y Colombia; lo cual no ocurre en el caso europeo, donde se restringe la protección a la persona física de manera exclusiva, tal como lo expresa el Reglamento UE 2016/679 en su artículo 1. En este sentido, una corriente de la doctrina (quienes no incluyen a las personas jurídicas dentro de la protección de datos personales) ha aceptado el criterio de que puedan reclamar por el uso indebido de la información relacionada con ellas, conjuntamente con los daños y perjuicios derivados de tales conductas, pero vistos desde la óptica del hecho ilícito. Y otro sector, se ha pronunciado por la incorporación de las personas morales dentro de esta protección, posición que consideramos más acertada.

> El amparo debido a los ciudadanos contra la posible utilización por terceros no autorizados, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte su entorno personal, social o profesional, en los límites de su intimidad.

Así pues, el derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar la esfera individual.

En este sentido, la protección de datos personales comienza a dar sus primeros pasos en Alemania, cuando en 1970 se promulga la *Datenschutz*, como la primera legislación en la materia, mediante la cual se pretendía dar protección a las personas naturales ante el riesgo que constituía el tratamiento sistematizado de datos nominativos por las autoridades gubernamentales.[13]

Los vertiginosos progresos informáticos dieron paso a un aumento de capacidad de acceso a la información, con la evidente necesidad de sistematizar su contenido a través de grandes bases de datos, que los legisladores europeos se vieron en la necesidad de regular, al tiempo que permitieron al titular de dichos datos la facultad de gozar de derechos de información, acceso, rectificación y cancelación sobre los datos obtenidos, manifestando un genuino interés por brindar garantías ante el tratamiento de los denominados "datos sensibles", entendidos como aquellos que por su naturaleza exigen un tratamiento más cuidadoso, ya sea porque lesionan potencialmente la intimidad de la persona, o bien porque la exponen a prácticas discriminatorias.

Lo que comenzó en Francia en 1978, se concretó inicialmente en Europa con el Convenio 108, adoptado por la Comunidad Económica Europea en 1981, figurando como el primer instrumento internacional que procuraba reglar el tratamiento automatizado de datos correspondientes a personas naturales, desde una perspectiva que trasciende la legislación interna y cuyo contenido influenció diversas legislaciones europeas de la época. El ámbito de aplicación del Convenio comprendía el procesamiento de datos desde su almacenamiento hasta el borrado, inclusive.

No obstante, con el paso del tiempo la eficacia del Convenio fue diluyéndose, dando paso a la Directiva 95/46/CE, que luego fue sustituida por el Reglamento UE 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de fecha 27 de abril de 2016, cuya aplicación comenzó el 25 de mayo de 2018.

---

[13] Cerda, Alberto. «Mecanismos de Control en la Protección de Datos en Europa.» *Ius et Praxis*, 2006: 221-251P.222.

Tanto la doctrina como la jurisprudencia y los textos constitucionales de países como Portugal, España, Hungría, Suecia, Finlandia y Venezuela, han reconocido la existencia de un derecho específico en relación con la protección de las personas ante el tratamiento de los datos personales que les conciernen, lo que en doctrina se alude como "autodeterminación informativa" o "libertad informativa"[14], cuya naturaleza es propia y separada del derecho a la intimidad, siendo ejercido bajo la figura del Habeas Data.

En la banca, la protección de datos se ve reflejada también en el establecimiento de registros de información crediticia o registros de solvencia que permiten a las instituciones bancarias obtener un perfil del individuo, con el objeto de valorar su calidad patrimonial y comportamiento crediticio, contexto en el cual debe respetarse al particular en la búsqueda de la estabilidad del sistema financiero y en el interés de encontrar mecanismos que faciliten el acceso al crédito.

"El cliente actual tiene un perfil más heterogéneo, más exigente, menos conformista, menos fiel, más voluble y más difícil de alcanzar.",[15] por lo que el afán de los bancos es garantizar tanto el cumplimiento de la ley como el innovar, a fin de dar un enfoque al cliente creando una experiencia grata, con una atención y servicio de calidad, pero sobre todo con garantías de seguridad en el manejo de la información.

Tal como se ha señalado, el derecho a la intimidad ha alcanzado en la sociedad de la información nuevos matices, lo que ha implicado que además del rechazo de invasiones en su ámbito privado, el individuo cuente con un derecho de control y acceso de toda información relativa a su persona, lo cual constituye un auténtico derecho fundamental protegido y garantizado constitucionalmente. Por tanto, resulta esencial para el titular de los datos personales recogidos, que se reconozcan y garanticen los derechos de información, acceso, rectificación, cancelación y objeción sobre dicha información. Estos derechos pueden desglosarse como:

a) Derecho a la información: contempla la comunicación al titular de los datos sobre el hecho mismo de la recolección, bien sea de forma directa o a través de terceros, con un detalle sobre las respectivas operaciones de tratamiento.

b) Derecho de acceso al interesado: a través de los cuales se le da la posibilidad al titular de acceder a los responsables del tratamiento, la finalidad de su procesamiento y el destino que se les dará, además de la lógica que subyace a todo tratamiento, resguardando debidamente el secreto comercial y respetando los derechos de propiedad intelectual relacionados.

---

[14] Cerda, Alberto. *Op.Cit*. P. 226.

[15] Hernández, Carlos, Raúl Arano, y Luis Cruz. «Estrategias aplicadas al Big Data para favorecer la atención en el servicio al cliente en empresas que ofrecen servicios financieros.» *Ciencia Administrativa*, 2020: 41-54. P.53.

Este derecho contempla además, la facultad personalísima que posee el titular de dirigir a la institución bancaria responsable del tratamiento, una solicitud de información relacionada con esta actividad.

c) Derechos de rectificación y cancelación: relacionados con los derechos de bloqueo y notificación a terceros a quienes se les hayan comunicado los datos antes de la rectificación, supresión o bloqueo de los mismos y representa la posibilidad del usuario de los servicios bancarios de exigir a la institución responsable del tratamiento que cumpla con el principio de calidad, corrigiendo cualquier error u omisión ajustando los datos obtenidos a la realidad o exigiendo la exclusión de los datos errados o en los cuales no tenga interés en que puedan ser tratados, ejerciendo lo que se conoce como derecho de cancelación.

d) Derecho del interesado a oponerse al tratamiento de ciertos datos que le conciernen y que no está interesado en divulgar.

e) La prohibición de que el titular sea sometido a decisiones con efectos jurídicos fundadas únicamente en un tratamiento automatizado de sus datos.

f) Derecho al olvido: referido a la supresión de los datos personales que hayan sido recolectados cuando se haya retirado el consentimiento otorgado inicialmente y no exista otro fundamento jurídico para que continúe su tratamiento; cuando ya no cumplan la finalidad para la cual fueron obtenidos, cuando el interesado se oponga al tratamiento y no subsistan motivos legítimos para ello, o cuando estos hayan sido obtenidos de manera ilícita o divulgados contra la voluntad de su titular.

Tal como puede observarse el derecho fundamental a la intimidad ha evolucionado hacia una concepción más amplia y dinámica que ha encontrado con el acceso a las nuevas tecnologías, nuevos mecanismos de protección, por cuanto consideramos que más allá del reconocimiento, es menester que se garanticen mecanismos que puedan hacer frente a su incorrecto uso y manejo.

2.1. Principios que orientan el tratamiento de datos

De acuerdo con Cerda[16] y Aponte[17], los principios asumidos por la antigua Directiva 95/46/CE que a nuestro criterio resultan perfectamente acogidos por el Reglamento UE 2016/679 y por lo tanto pueden considerarse aplicables por la banca para el tratamiento de datos personales, son los siguientes[18]:

---

[16] Cerda, Alberto. *Op. Cit*. P. 230 y ss.

[17] Aponte, Emercio. *Op. Cit*. P. 113 y ss.

[18] Véase *infra*, *3.1*. La Sala Constitucional del Tribunal Supremo de Justicia, en Sentencia N°1318, de fecha 04 de agosto de 2011, se pronunció sobre este particular al referirse a las instituciones del sector bancario y el procesamiento de datos personales.

a) Principio de licitud y lealtad: el tratamiento de datos personales de los usuarios del sistema bancario debe realizarse con estricto apego al ordenamiento jurídico y bajo los estándares de la buena fe.

b) Principio de información en la recolección de datos: corresponde a la banca, como responsable del tratamiento de los datos informar al titular, previo al tratamiento, sobre la existencia del mismo, su finalidad, destinatarios de la información, de la potestad que tiene el usuario de abstenerse a suministrar ciertos datos, si fuere el caso, y sus derechos de acceso, rectificación y cancelación al respecto.

c) Principio de la calidad de los datos: la información proporcionada por el usuario de los servicios bancarios debe representar fielmente la realidad que predica, guardando la pertinencia que se aparte de los excesos respecto al ámbito y objetivo para el cual fueron recolectados los datos, estando obligados los responsables de su tratamiento a velar por la exactitud y actualización de los mismos por el tiempo necesario para cumplir con la finalidad que motivó su registro.

La utilización de datos erróneos, puede afectar negativamente no sólo a los clientes, sino que también puede llegar a incumplir alguna regulación. En relación con las consecuencias negativas para los clientes sobre el manejo de información incorrecta, podría resaltarse el ejemplo de las empresas de generación de récords crediticios, conocidas como buró de crédito, que no hayan depurado correctamente la información obtenida de internet y que gracias a ello, perjudiquen a un determinado cliente.

d) Principio de consentimiento informado del titular de los datos: sólo puede efectuarse el tratamiento cuando el titular lo consienta expresamente, siendo informado de forma anticipada del propósito del almacenamiento de los datos y su posible comunicación a terceros. Admitiéndose la hipótesis de que puede prescindirse de tal consentimiento en atención a la fuente de la cual ha sido tomada la información o de los intereses individuales o sociales estimados prevalecientes, lo cual puede ocurrir en casos de recolección de datos para el ejercicio de actividades propias de la Administración Pública o cuando los datos procedan de una fuente pública.

Tal como destaca Aponte, el titular es el único con la facultad de decidir cómo, cuándo, dónde y quién trata sus datos personales, suministrando para ello una manifestación de su consentimiento que puede ser expresa, cuando se declara aceptar de forma transparente e inequívoca el tratamiento o cesión de sus datos, lo cual podría hacerse de forma verbal o escrita, mientras que el consentimiento tácito se puede inferir a través de la exteriorización de un comportamiento que demuestra aceptación, o a través del silencio o falta de oposición.[19]

[19] Aponte, Emercio. *Op. Cit*. P. 114.

e) Principio de la seguridad de los datos: el responsable de los datos deberá adoptar medidas de seguridad de diversa índole: físicas, referidas a la infraestructura que las resguarda, lógicas, con atención a las precauciones técnicas adoptadas (soporte, acceso, entre otras) y de índole normativo.

f) Principio de la confidencialidad de los datos: es la obligación de reserva respecto al contenido de la información procesada, la cual recae sobre el responsable del banco de datos y todas aquellos que intervienen en este proceso de manera directa; la cual subsiste después de la cesación de dichas funciones.

g) Principio de finalidad: si los datos fueron proporcionados por su titular, autorizando el tratamiento de los mismos con determinados objetivos, su uso para un fin distinto a este es ilegal, salvo excepciones legales en contrario.

h) Principio de especial protección a los datos sensibles: el tratamiento de este tipo de datos requiere de consentimiento expreso de su titular, en el entendido que dada la naturaleza de esta información, su conocimiento o divulgación puede atentar contra las libertades fundamentales o la intimidad de aquél a quien conciernen.

2.2. Riesgos a los que se encuentran sometidos los datos personales en la banca

Bajo la confianza que impera en las relaciones del usuario de productos financieros y la institución bancaria que ha seleccionado para depositar su dinero, el usuario entrega toda la información que le es requerida y en la actualidad, la tecnología ha abierto la puerta para que se puedan realizar distintas prácticas sobre los datos personales de un individuo. Sin embargo, el usuario desconoce en muchos casos el uso que se le pueda dar a dicha información y lo que no es menos importante, la afectación que pueda producirle las conclusiones que arroje el tratamiento de sus datos personales.

Debe constituir un compromiso y un deber serio para la banca desplegar todos los mecanismos necesarios para que su actividad no amenace ni lesione derechos humanos como la privacidad, la intimidad, la no-discriminación y la autodeterminación informativa.

El tratamiento inadecuado de datos personales suministrados por los usuarios, conduce a una serie de riesgos que el autor Nelson Remolina Angarita[20] analiza desde una óptica aplicable al caso colombiano. No obstante, la Profesora Nayibe Chacón Gómez durante su ponencia titulada “Ley sobre protección de datos y la contratación

[20] Remolina, Nelson. «Data Protection: riesgos y desarrollos (énfasis en el caso colombiano).» *Revista Chilena de Derecho Informático*, 2005: 111-134.

comercial: una tarea pendiente" dictada durante las VI Jornada de la Sociedad Venezolana de Derecho Mercantil, celebrada de manera virtual el 06 diciembre de 2023[21], consideró aplicables estos criterios a la situación venezolana actual, aportando una clasificación más resumida de los riesgos analizados, los cuales catalogó como: a) Riesgos en cuanto a la propia información; b) Riesgos de la tecnología; y c) Riesgo de ser víctima de delitos.

Respecto a la primera categoría de riesgos, se reconoce que el abanico de datos sobre una persona suele ser extenso e implicar una serie de datos que revelan información familiar, transacciones financieras, gustos, preferencias de compra, situación de salud, *hobbies*, procesos judiciales, condenas pernales, entrando además en el delicado concepto de los datos sensibles, donde se incluyen las creencias religiosas, las ideas políticas, e inclusive, las preferencias sexuales, lo cual podría producir consecuencias positivas o negativas para el titular de dicha información, de acuerdo a la identidad y objeto de quien realice el respectivo tratamiento.

Un dato que pueda ser catalogado como sensible para una persona, podría no serlo para otra y es que como acertadamente indicó la profesora Nayibe Chacón Gómez en la referida Jornada, un dato sensible podrá identificarse según su capacidad potencial de generar daño o no, a una determinada persona.

En la misma línea, se encuentra la publicación de información errónea, inexacta, incompleta, desactualizada o parcializada, lo cual comprometería directamente el honor, la reputación e inclusive hasta la libertad de un individuo. Cuando erróneamente se califica a un cliente como deudor en una base de datos, o se le mantiene en ella aún mucho tiempo después de haber cumplido con la totalidad de sus obligaciones, implica no sólo cerrarle las puertas del sistema financiero por tener un deficiente récord crediticio, sino afectar su honor, su credibilidad, desvaneciendo su solvencia injustamente.

Paradójicamente, sigue siendo una carga del ciudadano velar por la veracidad de la información de su propiedad que se encuentra en las más diversas plataformas y ejercer los mecanismos adecuados para que en caso de errores, sea rectificada o suprimida, lo que representa en muchos casos una gran brecha para el acceso a la justicia para quienes no posean el conocimiento o los recursos necesarios para llevar a cabo todas las actuaciones pertinentes, lo que representa a la fecha un desafío para el legislador venezolano.

---

[21] Chacón, Nayibe. «Ley de Protección de datos y la contratación comercial: una tarea pendiente.» *VI Jornada de la Sociedad Venezolana de Derecho Mercantil.* Caracas, 06 de diciembre de 2023. Video. https://www.youtube.com/watch?v=zqWWaNJQJno&t=4797s

Al hacer referencia al segundo grupo de riesgos, entendidos como riesgos de la tecnología o riesgos tecnológicos, resulta evidente la gran capacidad de los dispositivos, sistemas y la Big Data para almacenar y procesar información de la más variada índole, lo cual ha aumentado considerablemente desde el surgimiento del uso masivo de la inteligencia artificial y la facilidad que existe actualmente para acceder a todo este torrente de información, riesgo que aumenta cuando un solo dato podría permitir la interconexión de muchas otras bases de datos, revelando una copiosa cantidad de información sobre la persona de su titular.

El cruce de esa información podría generar lo que Remolina Angarita denomina un "perfil virtual"[22], que el receptor de esos datos podría construir sobre un determinado individuo, lo que sería positivo o perjudicial, de acuerdo al tipo de información y la exactitud que posea.

Al hablar sobre el tercer grupo de riesgos, es decir, los riesgos a ser víctima de delitos, la banca encuentra en esta categoría su aspecto más vulnerable en cuanto al tratamiento de datos personales, pues resulta obvio que una institución financiera conserva información certera de la cantidad de dinero que cada uno de sus clientes posee, los movimientos que realiza, sus gustos, preferencias, patrones de consumo, entre otros que se han mencionado en el curso de esta investigación.

El crecimiento descontrolado de la información disponible ha provocado un aumento de la complejidad y sofisticación de los mecanismos del crimen organizado y las actividades fraudulentas, lo que obliga a los bancos a realizar la dura tarea de detectar el fraude bancario en internet, mejorando los procesos de análisis de la información y utilizando mecanismos de ciberseguridad que optimicen la prevención de ataques de hackers, el ciberespionaje, utilización de *phishing*, *ransomware*, entre otros, a través de la identificación temprana de lagunas, fortalezas, debilidades y riesgos de sus sistemas en línea, máxime cuando la comisión de delitos informáticos sirve de puente para otros delitos, tales como la piratería, la extorsión, sustracción de fondos de las cuentas bancarias y demás prácticas de corrupción.

Las instituciones financieras buscan proporcionar seguridad a sus clientes y dar máxima prioridad al control de sus productos, debido al creciente fraude financiero. Ahora más que nunca, los bancos han puesto regulaciones en cuanto a la verificación de la identidad de todos sus clientes, ya que el robo de identidad también es una de las mayores fuentes de fraude y de brecha de los sistemas informáticos.

---

[22] Remolina, Nelson. *Op. Cit*. P.122.

La banca tiene el deber de proteger la información que le ha sido confiada y que de primera mano obtiene, a fin de que evitar que sus clientes y relacionados sean objeto de extorsiones, sabotajes, discriminaciones, amenazas o daños a su patrimonio o a su vida, derivados de un tratamiento negligente de la información que poseen en calidad privilegiada. En caso de robo de datos, la respuesta del banco debe ser efectiva, actuando tanto a petición del usuario como de manera autónoma al detectar actividades sospechosas, notificando al usuario afectado, quien deberá decidir si los hechos configuran o no, un caso sospechoso para activar las medidas correspondientes en caso de serlo[23].

El manejo de los datos personales por la banca, deberá hacerse bajo el marco de la responsabilidad, a fin de impedir su alteración, pérdida, acceso o tratamiento no autorizado, donde constituya un auténtico deber la constante actualización de datos financieros relativos al récord crediticio, historial de pagos, entre otros aspectos, cuya falta de veracidad pudieran producir un perjuicio al cliente, por lo que deberá darse información veraz y oportuna al interesado sobre el contenido de los datos almacenados y el respectivo uso que se les dará, actuando aún de oficio para corregir la información errónea, incompleta o vetusta, capaz de afectar al particular en el ejercicio de sus actividades.

Asimismo, resulta evidente que una nueva Ley de Protección de Datos deberá establecer severas responsabilidades civiles, penales y administrativas para las instituciones que ejecuten un tratamiento irresponsable de la información suministrada, entendiendo siempre que es la persona y no el banco, el titular de dichos datos individuales.

Es oportuno señalar que los daños que puedan sufrir las personas titulares de datos personales han de ser reparados por el responsable del tratamiento de datos; el cual sólo podrá ser eximido de responsabilidad si se demuestra que no le es imputable el hecho que ha provocado el daño, bien sea por la responsabilidad del propio interesado o por un caso de fuerza mayor, con la oportuna aplicación de sanciones para los responsables.

Como puede verse, lo que se persigue no es otra cosa que un tratamiento ético y responsable de datos rodeado de todas las garantías que protejan al usuario de los servicios bancarios en el pleno goce y ejercicio de sus derechos fundamentales a la intimidad, privacidad y autodeterminación informativa, sin que se le exponga injustamente

---

[23] En julio de 2023, el diario El Nacional publicó un artículo donde se hacía referencia a un presunto ataque cibernético sufrido por el Banco de Venezuela, mediante el cual un grupo de piratas informáticos se atribuía el robo de la data sobre los clientes del banco. A su vez, la entidad financiera negó la veracidad de tales hechos, manifestando que sus plataformas operaban con normalidad, sin que ello privara a los particulares de sentir temor por el riesgo a la exposición de su información personal. Véase: De Jesús, Luis: "Hackers publicaron datos confidenciales de clientes del Banco de Venezuela", El Nacional, 14 de julio de 2023, https://www.elnacional.com/venezuela/hackers-publicaron-datos-confidenciales-de-clientes-del-banco-de-venezuela/.

a riesgos, discriminaciones o a ser víctima de actividades delictivas, entendiendo que no puede pretenderse que deje de usarse la tecnología para la recolección de datos que beneficien a las empresas y produzcan un aumento de la generación de empleos, del crecimiento económico y la libre competencia para proporcionarle a los ciudadanos el disfrute de servicios bancarios de la mejor calidad y con la mayor transparencia.

3. El caso venezolano: el procesamiento de datos y la protección al usuario del sistema bancario

Aunque la protección de datos en Venezuela carece de regulación propia con normas de carácter específico, constitucionalmente la protección de datos y acceso a la información se consideran derechos fundamentales. El punto de partida es el artículo 28 de la Carta Magna:

> Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.

Además, el artículo 60 establece que:

> Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.

Del contenido de los artículos anteriores se infiere, -*grosso modo*-, lo siguiente:

1. Que la protección de datos es un derecho fundamental de carácter personalísimo basado en la protección del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de los individuos.
2. Que toda persona tiene el derecho de acceder a la información que sobre sí mismo conste en registros oficiales o privados.
3. Que toda persona tiene el derecho de saber la finalidad para la cual fueron recabados sus datos y el uso que se les dé a los mismos.
4. Que la misma Constitución establece los límites a su ejercicio al señalar que hay determinadas restricciones a este derecho de acceso a la información.

5. Que la competencia para el ejercicio efectivo del derecho a la protección de datos personales le corresponde a los Tribunales de la República. Ergo, su protección es jurisdiccional y no administrativa, sin que ello signifique negar la posibilidad de materialización de este último supuesto.

Y esto se concatena con el artículo 143 *ejusdem*:

> Los ciudadanos y ciudadanas tienen derecho a ser informados e informadas oportuna y verazmente por la Administración Pública, sobre el estado de las actuaciones en que estén directamente interesados e interesadas, y a conocer las resoluciones definitivas que se adopten sobre el particular. Asimismo, **tienen acceso a los archivos y registros administrativos, sin perjuicio de los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto**. No se permitirá censura alguna a los funcionarios públicos o funcionarias públicas que informen sobre asuntos bajo su responsabilidad. (Destacado nuestro).

Con este basamento constitucional, surgieron una serie de leyes y normas posteriores, que, si bien no regulan las mismas materias, coinciden en integrar los principios de conocimiento de la información, confidencialidad de la información, protección de datos y límites en el uso de la información de los particulares. Propicio resulta mencionar a la Ley Orgánica del Tribunal Supremo de Justicia[24], que establece que:

> Artículo 167: Toda persona tiene derecho a conocer los datos que a ella se refieran así como su finalidad, que consten en registros o bancos de datos públicos o privados; y, en su caso, exigir la supresión, rectificación, confidencialidad, inclusión, actualización o el uso correcto de los datos cuando resulten inexactos o agraviantes. El Habeas Data sólo podrá interponerse en caso de que el administrador de la base de datos se abstenga de responder el previo requerimiento formulado por el agraviado dentro de los veinte días hábiles siguientes al mismo o lo haga en sentido negativo, salvo que medien circunstancias de comprobada urgencia.

Tal como se observa, el primer aparte de este artículo desarrolla de forma cónsona con la Carta Marga el derecho al acceso a los datos personales, mientras que, el segundo aparte abarca el mecanismo de protección de los datos personales cuando se presuma su agravio, que consiste en la acción judicial de Habeas Data, en el que ahondaremos seguidamente.

---

[24] Gaceta Oficial N° 6.684 Extraordinario, de fecha 19 de enero 2022.

3.1. Habeas data en la Sentencia SCTSJ N°1318 de fecha 04 de agosto de 2011

La Sala Constitucional del Tribunal Supremo de Justicia en sentencia N°1318 del 04 de agosto 2011 (en lo adelante, SCTSJ N°1318 04/08/2011), fijó el criterio vinculante en cuanto a la protección de datos en materia bancaria, desarrollando el contenido del ejercicio del Habeas Data y haciendo especial referencia al Sistema de Información Central de Riesgos (SICRI).

Señala esta sentencia que la protección de datos de carácter personal constituye un derecho fundamental autónomo cuya finalidad es permitir que todas las personas puedan controlar el acceso y uso por terceros de sus datos personales y, a su vez, evitar que los datos de carácter personal recogidos sufran desviaciones de la finalidad para la que fueron recabados.

A su vez, el juzgador hace referencia a la sentencia N° 332/01, en la que se analiza que el precitado artículo 28 constitucional otorga dos derechos simultáneos: En primer lugar, el derecho que posee el individuo de acceder a la información y a los datos que sobre sí misma o sus bienes consten en registros oficiales o privados y en segundo lugar, al derecho de conocer la finalidad y uso que da el compilador a estos datos e informaciones, reconociendo a su vez el derecho implícito contenido en la norma de recopilar información sobre las personas y sus bienes.

El juzgador avanza extendiéndose hacia la interpretación del *habeas data*, precisando que el ejercicio de las acciones derivadas del mismo no funcionan en relación a expedientes de trabajos que reposan en un archivo, a datos sueltos o anotaciones en papeles domésticos o comerciales, sino que opera en cuanto a sistemas (no sólo informáticos) que organicen por cualquier método la información relativa a las personas o sus bienes, para un beneficio particular o de terceros y que pudieran resultar perjudiciales contra aquellos a quienes se refiere la recopilación. Se trata entonces de bancos de datos ordenados de forma tal que permitan hacer un perfil de las personas, sus actividades o sus bienes, destinados a inscribir documentos, operaciones o actividades de las personas en determinados campos capaces de determinar ciertos patrones.

Del análisis de esta decisión jurisprudencial, se extraen cinco supuestos generales que deben materializarse para que pueda ser ejercido el *habeas data*:

1. Que la recopilación de datos no sea aislada, mental o tenga como fin su uso personal, de estudio, cultural o espiritual.
2. Que la recopilación de datos tenga como fin obtener información general sobre una persona, sus bienes o actividades, organizados de forma sistemática y que permitan elaborar perfiles sobre los titulares de los datos, bien sea por si sola o entrecruzada con otras bases de datos.

3. Que la información debe, necesariamente, estar organizada sistemáticamente, más no obligatoriamente a través del uso de la informática.
4. Que el uso de la información recopilada sobre una persona sea o pueda ser perjudicial contra sí misma.
5. Que el ejercicio del *habeas data* no constituye una violación del derecho a la privacidad, ya que respecto a este último se aplican las limitaciones reconocidas por la ley.

Retomamos el análisis del juzgador en la SCTSJ N°1318 04/08/2011, que expresamente sobre la materia bancaria advierte lo siguiente:

> (…) la regulación no va dirigida exclusivamente a la actividad de los órganos y entes públicos, sino por igual a la actividad desarrollada por particulares que se vinculen o incida sobre el derecho a la protección de datos personales como por ejemplo puede evidenciarse, en el sector bancario, que cuentan con un Sistema de Información Central de Riesgos, pero el cual no constituiría una garantía real para los usuarios, si sistemas de información paralelos, como los denominados "burós de crédito o sociedades de reportes del consumidor privadas" no ofrecen una protección debida de los datos, bajo los siguientes principios.

Esta precisión reafirma la responsabilidad de las instituciones del Sector Bancario e instituciones paralelas de contar con sistemas orientados a la protección de datos, específicamente en el Sistema de Información Central de Riesgos, objeto de consulta por todas las instituciones bancarias. Estos sistemas de bases de datos personales deben contar con una serie de garantías concretas, y así lo expresa el aludido fallo cuando reconoce que del Texto Constitucional derivan las condiciones mínimas de garantía relativas al derecho a la protección de datos personales, las cuales resultan aplicables en términos generales a todos los sistemas de bases de datos personales que sean objeto de tratamiento electrónico o no, salvo las excepciones que al efecto establezca la ley.

Las garantías a las que se refiere este fallo corresponden a los principios que orientan el tratamiento de datos personales de acuerdo con la legislación europea y de la mayoría de los países que cuentan con legislaciones específicas en la materia, las cuales, como se indicó previamente, responden a los parámetros relativos al principio de autonomía de la voluntad o del consentimiento previo, libre, informado, inequívoco y revocable para el tratamiento de datos personales; el principio de legalidad que permita la recopilación de datos; el principio de finalidad y calidad, que orienta una causa de recopilación con apego a las leyes y la exactitud, vigencia y veracidad de la información recabada.

La Sala hace énfasis en el principio de temporalidad, que exige que la conservación de los datos personales se extienda hasta el logro de los objetivos que justificaron su obtención y tratamiento, que en materia bancaria se aplica en los casos donde un

particular ha incurrido en mora o retardo en el cumplimiento de una obligación crediticia y se le incluye en el Sistema de Información Crediticia (SICRI) como "deudor moroso", pero de acuerdo al cual, una vez realizado el pago de las respectivas acreencias debe ser retirado de tales registros, en sintonía con lo planteado por la Sentencia de la Sala Constitucional N°4.796/07, que subraya el derecho de toda persona a que la información que sobre sí misma se recoja en cualquier base de datos pública o privada, sea debidamente actualizada inclusive de oficio.

Por otra parte, el principio de exactitud y de autodeterminación le da relevancia al manejo de datos exactos, completos y actualizados con procedimientos claros que le permitan al titular determinar el tratamiento que reciben tales informaciones, la finalidad de su recopilación, teniendo la posibilidad de solicitar en todo momento su actualización, rectificación o eliminación, haciéndola del conocimiento de todos aquellos que tuvieron la oportunidad de conocer la información errónea.

Con respecto al principio de previsión integralidad o el conocimiento del titular sobre toda la información que repose en todos aquellos sistemas de recopilación que contengan datos sobre una misma persona, la Sala manifestó en relación al Sistema de Información Central de Riesgos, el deber de incluir además de los usuarios que representan "sujetos riesgosos" según los criterios de la legislación financiera, a aquellos sujetos que mediante sentencia definitivamente firme, hayan sido condenados por delitos que atenten contra la integridad en el desarrollo de una actividad económica, como la bancaria o financiera, lo que se extiende a aquellas personas sometidas a intervenciones o procesos de liquidación.

El sentenciador alude además al principio de seguridad y confidencialidad, impidiendo la alteración de datos por terceros y el acceso no autorizado a los mismos. Asimismo, enfatiza el principio de tutela, que reconoce la necesidad de que los titulares sean provistos de mecanismos judiciales y extrajudiciales que garanticen su derecho a la protección de datos, con una respuesta oportuna, que en atención al principio de responsabilidad, sancione proporcionalmente de manera civil, penal y administrativa a quienes hayan realizado un tratamiento negligente de los datos suministrados

3.2. Sistema de Información Central de Riesgos (SICRI)

El Sistema de Información Central de Riesgos (en lo adelante, SICRI), se encuentra regulado en el artículo 88 de la Ley de Instituciones del Sector Bancario, como:

> (…) una base de datos o registro de la actividad crediticia del sector bancario nacional bajo la responsabilidad de la Superintendencia de las Instituciones del Sector Bancario, el cual permite consultar la situación crediticia de los distintos usuarios y usuarias de las instituciones y cuya finalidad es precisar los niveles de riesgo.

Como bien lo precisa el primer apartado del artículo, es una base de datos que recopila la información crediticia de distintos usuarios y que podrá ser utilizada por las instituciones que componen al Sector Bancario exclusivamente para asignar niveles de riesgo según los procedimientos establecidos para tal actividad. Es decir, no podrá ser utilizada la información allí contenida para fines diferentes, como la negación de productos o servicios financieros.

Todas las entidades reguladas por la citada ley están en la obligación de proporcionar la información necesaria para complementar la base de datos, a fin de recopilar información adicional para facilitar la evaluación de riesgos, contribuir con las normas de identificación del usuario y usuaria para la prevención de legitimación de capitales y financiamiento al terrorismo, y facilitar el acceso a productos crediticios a las personas sin historial bancario según el juicio del ente regulador; y así lo expresa el artículo 89 *ejusdem*. Como garantía al derecho de protección de datos, -médula espinal de las instituciones financieras-, en el mismo artículo se le otorga potestad a la SUDEBAN para suministrar la información contenida en el SICRI a los usuarios afectados.

Como corolario de lo anterior, las instituciones financieras tienen prohibido informar a otras personas, naturales o jurídicas, así como a Organismos Públicos o Privados, salvo que sea al mismo usuario, a la Superintendencia correspondiente, al Banco Central de Venezuela y demás entes autorizados expresamente por la Ley de Instituciones del Sector Bancario, salvo que el usuario dé autorización escrita que autorice su difusión, que él mismo podrá revocar posteriormente (art. 90). A esta prohibición la ley la denomina como "prohibición de informar" y no es más que la concreción de las garantías de los principios de la autonomía de la voluntad, legalidad, seguridad y confidencialidad.

3.3. Aplicación del régimen sobre la protección de datos de los usuarios en la banca

El Sector Bancario ha procurado regular la protección de datos de los usuarios a través de disposiciones contenidas en diversas normas. Ese interés sectorial se debe al alto flujo de datos masivos o Big Data que se genera a partir del uso, -por parte de los personas naturales y jurídicas-, de los servicios bancarios y demás servicios conexos ofrecidos las instituciones financieras de esta naturaleza, cuya recolección inicia en el momento en el que se efectúa el *Onboarding* y se mantiene en constante actualización. Para conocer de qué manera el Sector Bancario regula la materia, es menester partir de la Ley de Instituciones del Sector Bancario, que en su artículo 86 regula el sigilo bancario.

> Artículo 86: Está prohibido a las instituciones bancarias, así como a sus directores o directoras y trabajadores o trabajadoras, suministrar a terceros cualquier información sobre las operaciones pasivas y activas con sus usuarios y usuarias, a menos que medie autorización escrita de éstos o se trate de los supuestos consignados en el artículo 87 del presente Decreto con Rango, Valor y Fuerza de Ley. (...)

Empero, el secreto bancario no es absoluto ya que la misma ley en su artículo 87 establece sus limitaciones.

A juzgar por la disposición anterior, podría pensarse que el alcance de la protección de datos se limita exclusivamente a la información relacionada a las operaciones pasivas y activas de los usuarios. No obstante, a nuestro modo de ver resulta errónea esta restrictiva línea de pensamiento ya que existe un conjunto de normas emanadas de la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN) que perfilan, -o complementan, si se quiere- este concepto.

Es en el año 2010, con la Resolución Nro. 641-10 del 23 de diciembre, en la que se publican las Normas que Regulan el Uso de los Servicios de la Banca Electrónica, cuando se define a detalle qué debe entenderse por "dato sensible". Según el artículo 2 de esta norma, debe entenderse por dato sensible: "Datos con carácter confidencial del cliente y/o usuario de la Banca Electrónica, tales como número de cuenta; número de identificación personal; claves del cliente; número de tarjeta; código de seguridad de la tarjeta.".

Aunque el ámbito de aplicación de la norma en cuestión se extiende a los servicios de Banca Electrónica, es necesario hacer una interpretación integradora con el artículo 86 de la Ley de Instituciones del Sector Bancario para ampliar tanto su conceptualización como su alcance a todo el compendio de servicios ofrecidos por la banca. De este modo, puede extenderse el ámbito de protección a la mayor cantidad de información contenida en las bases de datos de las instituciones financieras, para que, por un lado, los titulares de los datos personales puedan ejercer sus derechos derivados de esta protección, y, por el otro, que esta información sea manejada con la mayor cautela posible por las instituciones de modo que sea utilizada estrictamente para los fines para los cuales fue recabada.

En la Resolución Nro. 063 de fecha 12 de junio de 2015, contentiva de las Normas Relativas a la Protección de los Usuarios de los Servicios Financieros, se obliga a los sujetos regulados a salvaguardar los datos personales e información de los productos o servicios mantenidos o que hayan mantenido los usuarios y clientes, así como el manejo de esta información con estricta confidencialidad (artículo 16). También se prohíbe "intercambiar o compartir por cualquier medio las resultas o cualquier información de las solicitudes de financiamiento o crédito, formulados por clientes, usuarios y usuarias que hayan sido negadas en cualquier instancia." (artículo 58).

Existen también las Normas que regulan el uso de Tecnología Financiera del Sector Bancario, las llamadas FINTECH[25], entendidas como un conjunto de disposiciones cuya finalidad principal es "regular los servicios financieros prestados a través de nuevas tecnologías, ofrecidas por Instituciones de Tecnología Financiera en cualesquiera de sus modalidades, a las Instituciones del Sector Bancario; así como su organización, operación y funcionamiento" (Artículo 1).

Si bien su norte principal es regular el uso de las nuevas tecnologías en la banca, el desarrollo de nuevos productos distintos a los servicios tradicionales en aplicación de nuevas tecnologías y el armónico desenvolvimiento de los proveedores de dichos servicios financieros, de alguna manera también responden al deber de proteger la información de los usuarios a través de la implementación de diversos protocolos de seguridad para evitar la fuga de información, transmisión de información de forma inapropiada o indebida, confidencialidad de información o datos sensibles, y salvaguardar la integridad del usuario. Esto se evidencia en varias de sus disposiciones, comenzando por el artículo 3, numeral 20, que define los Datos Masivos:

> También llamados agregadores de datos, macrodatos, inteligencia a gran escala o datos a gran escala es un término que hace referencia a conjuntos de datos tan grandes y complejos que precisan de aplicaciones informáticas no tradicionales de procesamiento de datos para tratarlos adecuadamente.

Por su parte, el artículo 17, numeral 5, exige a las Instituciones de Tecnología Financiera del Sector Bancario (ITFB), desarrollar procesos de seguimiento y revisión de productos, servicios o canales de entrega, que permitan, entre otras cosas velar por el cumplimiento de los requisitos relativos a la protección de datos y protección a los consumidores; más adelante, en consonancia con el artículo anterior, el artículo 23 en sus literales l y m, exigen expresamente que las ITBF cuenten con elementos de seguridad para el acceso a los clientes para evitar vulneraciones e implementar sistemas de cifrado en la transmisión y sistemas de información sensible de los clientes para evitar su conocimiento por terceros no autorizados.

Recientemente, la SUDEBAN publicó una circular que reglamenta el uso de los servicios de computación en la nube[26]. Esta norma resulta importante para este estudio ya que regula detalladamente el uso de los servicios de computación en la nube en los servicios bancarios y conexos. Pero antes de avanzar con estos lineamientos, es imprescindible entender qué es la computación en la nube y cuáles son sus aplicativos. El

---

[25] Resolución N°001.21 de fecha 04 de enero de 2021, contentiva de las normas que regulan los servicios de tecnología financiera (FINTECH), publicada en la Gaceta Oficial N°42.162, de fecha 06 de julio de 2021.

[26] SUDEBAN. Circular N°SIB-II-GGIR-GRT-GGR-GNP-08724, de fecha 29 de diciembre de 2023.

National Institute of Standards and Technology (NIST) y su Information Technology Laboratory[27], la computación en la nube se define como:

> Un modelo que permite el acceso bajo demanda a través de la red a un conjunto compartido de recursos de computación configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar rápidamente con el mínimo esfuerzo de gestión o interacción del proveedor del servicio.

¿Cuál es la relación entre la computación en la nube y la Big Data? La computación en la nube permite el almacenamiento de información en servidores alojados en internet, los cuales gozan de una amplia capacidad, así como flexibilidad y escalabilidad en el uso de los servicios, características que facilitan el almacenamiento de una mayor cantidad de datos (Big Data) y agilizan su análisis.

Ahora bien, precisado el concepto de la computación en la nube y su utilidad, resulta propicio volver a la circular que regula el uso de la computación en la nube de la SUDEBAN. En sus consideraciones previas, el ente regulador expresa su preocupación sobre los riesgos potenciales que supone el uso de la computación en la nube ya que "podrían vulnerar los principios fundamentales de la seguridad de la información relativos a la confidencialidad, integridad y disponibilidad de los datos, en especial a los inherentes a las bases de datos de clientes y la información financiera de los Sujetos Obligados*"*. Válida resulta tal preocupación ya que, por su característica de uso común y virtualización, es posible que si no se utilizan proveedores de computación en la nube con altos estándares de seguridad, la información podría ser vulnerada.

En consecuencia, el ente regulador exige que los proveedores de servicios de computación en la nube que presten servicios a las Instituciones Bancarias deben estar domiciliados en el territorio nacional; la novedad resulta la prohibición implícita del uso de los servicios de computación en la nube a través de proveedores no domiciliados en el país, como, por ejemplo, Amazon Web Service o Azure, siendo estos dos de los proveedores más recurrentes en este tipo de servicios. La intención de esta exigencia es evitar el almacenamiento de información sensible fuera de nuestro territorio y su uso indebido bajo el amparo de otras legislaciones que quizás no contemplen en su sistema jurídico la protección de datos personales. Otro requerimiento relacionado es el de proteger la información sensible con procesos de generación, transmisión y almacenamiento con el uso de algoritmos cifrados y que el acceso a la base de datos, aplicaciones y sistemas no deberá delegarse en terceros contratados.

---

[27] Mell, Peter; Grance, Tim, Effectively and Securely Using the Cloud Computing Paradigm (National Institute of Standards and Technology (NIST), mayo de 2009), XXXX, https://csrc.nist.gov/CSRC/media/Presentations/Effectively-and-Securely-Using-the-Cloud-Computing/images-media/fissea09-pmell-day3_cloud-computing.pdf.

Si bien nuestra legislación resulta un poco escueta en la regulación sobre la protección de datos, hay que reconocer que el Sector Bancario ha hecho un gran esfuerzo en desarrollar con la mayor precisión posible un sistema que permita la protección los datos e información, no solo de sus usuarios sino de los sujetos obligados. Se persigue la confidencialidad, el resguardo de la información a través de sistemas y medios informáticos específicos que gocen de protocolos de seguridad robustos, a los fines de evitar la utilización de la información contenida en sus grandes bases de datos de forma inapropiada, así como su fuga o pérdida todo ello de conformidad con el marco constitucional en la materia. Sin embargo, no existe un procedimiento administrativo específico por si llegase a materializarse estos últimos supuestos, quedando a discreción del ente regulador cual deberá ser el proceder en estos casos.

Así las cosas, tampoco existe un procedimiento administrativo para que los usuarios titulares de los datos formulen denuncias en caso de que la información contenida sobre su persona en las Instituciones Bancarias sea mal utilizada, distribuida, publicada o modificada sin su autorización. No obstante, lo anterior no implica la anulación del derecho de los particulares a solicitar administrativamente la garantía o restitución de sus derechos relacionados con la protección de datos y acceso a la información, como tampoco implica que el ente regulador goce del derecho a negarse a responder dichas solicitudes sólo por la inexistencia de un procedimiento específico, ya que esto significaría negar los derechos fundamentales recogidos en nuestra Carta Magna y además, sería totalmente opuesto a las obligaciones del ente regulador, específicamente en cuanto a proteger los intereses del público se refiere.

CONCLUSIONES

Por su actividad de intermediación dentro del Sistema Financiero, la banca cuenta con el acceso a grandes volúmenes de información sobre sus clientes y relacionados, para cuyo análisis ha recurrido a la Big Data, a fin de obtener mejores resultados en calidad de productos y servicios enfocados en las necesidades de su clientela lo que a su vez, le reporta grandes beneficios. Sin embargo, el usuario del sistema bancario es el verdadero titular de toda la información suministrada y cuenta con derechos fundamentales que abarcan el compás de los principios que orientan su tratamiento y ponen sobre la banca el compromiso ineludible de hacer frente a los riesgos que pueda acarrear un uso negligente de la información que debe procesar de manera ética y responsable, para evitar la exposición de los particulares al fraude informático, reduciendo el margen de acción para el crimen organizado, el financiamiento al terrorismo y demás delitos conexos.

En Venezuela, la Constitución de 1999 incluyó a la protección de datos como el derecho de autodeterminación informativa, como una esfera individualizada del derecho a la intimidad. Sin embargo, hasta la fecha no hay un desarrollo legislativo sobre la materia, más allá de algunas disposiciones aisladas dentro del ordenamiento, lo cual sigue constituyendo una mora del legislador para con los particulares.

No obstante lo anterior, la Jurisprudencia del Tribunal Supremo de Justicia ha partido de un reconocimiento expreso a los derechos fundamentales en esta materia, haciendo oportuna mención a los principios que deben regir la conducta de las entidades bancarias en cuanto al tratamiento de datos personales se refiere y a su vez, estableciendo los límites de la utilización del Sistema de Información de Riesgos (SICRI), cuyo empleo no podrá darse para estigmatizar al individuo negándole el acceso a créditos u otros productos financieros, preservando además el derecho del particular a solicitar la supresión de datos erróneos, vetustos o incompletos que puedan perjudicarle.

El contenido de diversas Resoluciones y Circulares de la SUDEBAN, reconoce la existencia de tales derechos y procura perfilarlos a la par de las nuevas empresas de servicios de tecnología financiera; mientras que el Sector Bancario tradicionalmente ha realizado loables esfuerzos orientados al mantenimiento de buenas prácticas que protejan los datos personales de los particulares, hasta tanto surja una nueva legislación que sitúe a Venezuela en una posición de verdadero compromiso ante la protección de los matices que el uso de las nuevas tecnologías seguirá aportando al óptimo ejercicio de los Derechos Humanos.

BIBLIOGRAFÍA

Aponte, Emercio. «La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano.» *Revista de Derecho Privado. Universidad Externado de Colombia*, 2007: 109-124.

Banco de Venezuela. *Informe Primer Semestre 2022.* Caracas: Banco de Venezuela, 2022 https://www.bancodevenezuela.com/files/informesgestion/Memoria%20(informe%20Junta%20directiva)I%20Semestre%202022.pdf.

Cerda, Alberto. «Mecanismos de Control en la Protección de Datos en Europa.» *Ius et Praxis*, 2006: 221-251

Chacón, Nayibe. «Ley de Protección de datos y la contratación comercial: una tarea pendiente.» *VI Jornada de la Sociedad Venezolana de Derecho Mercantil.* Caracas, 06 de diciembre de 2023. Video. https://www.youtube.com/watch?v=zqWWaNJQJno&t=4797s

Chacón, Nayibe. «Reseña histórica de la protección al consumidor y usuario en Venezuela: Mucho más que "precios justos".» *Revista Venezolana de Legislación y Jurisprudencia N° 9*, 2017: 141-165.

Cueto, Marta. «Big Data en la banca y sus implicaciones para el futuro.» *Trabajo de Grado. Universidad Pontificia Comillas.* Madrid, 2019.

De Jesús, Luis. «Hackers publicaron datos confidenciales de clientes del Banco de Venezuela.» *El Nacional*, 14 de 07 de 2023.

https://www.elnacional.com/venezuela/hackers-publicaron-datos-confidenciales-de-clientes-del-banco-de-venezuela/.

García, Aristeo. «La protección de datos personales: derecho fundamental del siglo XXI un estudio comparado.» *Boletín Mexicano de Derecho Comparado*, 2007: 743-778.

Hernández, Carlos, Raúl Arano, y Luis Cruz. «Estrategias aplicadas al Big Data para favorescer la atención en el servicio al cliente en empresas que ofrecen servicios financieros.» *Ciencia Administrativa*, 2020: 41-54

Mell, Peter; Grance, Tim, Effectively and Securely Using the Cloud Computing Paradigm (National Institute of Standards and Technology (NIST), mayo de 2009), PP.69, https://csrc.nist.gov/CSRC/media/Presentations/Effectively-and-Securely-Using-the-Cloud-Computing/images-media/fissea09-pmell-day3_cloud-computing.pdf

Red Iberoamericana de Protección de Datos. «Estándares de Protección de Datos Personales.» 2017. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

Remolina, Nelson. «Data Protection: riesgos y desarrollos (énfasis en el caso colombiano).» *Revista Chilena de Derecho Informático*, 2005: 111-134.

S/A. Big Data: "¿En qué consiste? Su importancia, desafíos y gobernabilidad". Power Data, 2023 *Power Data.* 2023. https://www.powerdata.es/big-data. (último acceso: 04 de 12 de 2023).