Universidad del Azuay

Facultad de Ciencias Jurídicas

Escuela de Derecho

RESPONSABILIDAD BANCARIA: MANEJO DE DATOS PERSONALES Y LA VIOLACIÓN A LA PRIVACIDAD DEL DEUDOR

Autor:
Lucía Bernarda Abdo León

Director:
Esteban Francisco Coello Muñoz

Cuenca – Ecuador
2024

DEDICATORIA

María Teresa León, Diego Cabezas y Amelia Cabezas, las tres personas que más amo en la vida.
Mi más grande inspiración

AGRADECIMIENTO

Esteban Coello, La persona que más ha marcado mi carrera universitaria, mi ejemplo a seguir y la inspiración para convertirme en el profesional que aspiro ser.

Diego Idrovo, Luis Sánchez y Wilson Villavicencio, Mis tres grandes mentores, aquellos que la vida me ha regalado, son mí mayor impulso para crecer como profesional.

RESUMEN:

El derecho a la privacidad y la protección de datos en el ámbito financiero ecuatoriano es fundamental. Existe una regulación del tratamiento de la información personal que interactúa con los derechos constitucionales. La investigación se centra en el manejo de la información crediticia y personal por parte de las entidades financieras, especialmente en el contexto de los procedimientos de cobro, donde el sigilo bancario constituye un elemento fundamental para preservar la confianza en la relación usuario-entidad. Estableciendo así que las entidades financieras no tienen responsabilidad por el manejo de datos personales, mas, existen terceros encargados del proceso de cobro de obligaciones que hacen un uso inadecuado de los mismos, comprometiendo su adecuada protección. En la Constitución de la República del Ecuador, el Código Orgánico Monetario y Financiero, y la Ley Orgánica de Protección de Datos Personales, se destacan los principios de transparencia, confidencialidad y legalidad como elementos esenciales para la adecuada gestión de los datos de los usuarios financieros. Incluyendo un estudio de los contratos de adhesión, característicos en el sector financiero, en los cuales se imponen condiciones sin posibilidad de negociación, pero que deben respetar la protección de los derechos de los consumidores. Además, dentro de esta investigación se resalta la importancia de implementar políticas de privacidad y fomentar un marco legal que limite el acceso no autorizado a datos financieros sensibles. Finalmente, se presenta un análisis internacional comparado sobre protección de datos financieros, destacando el equilibrio de la seguridad de la información con el derecho a la privacidad.

Palabras clave: Derecho-privacidad , Protección-datos, Confidencialidad, Entidades financieras, Contratos- adhesión.

ESTEBAN FRANCISCO COELLO MUNOZ

Digita lly sign e d by ESTEB AN FRANCISC O COELLO MUNO Z
Date : 2024.11.15 10:34:12 -05'00'

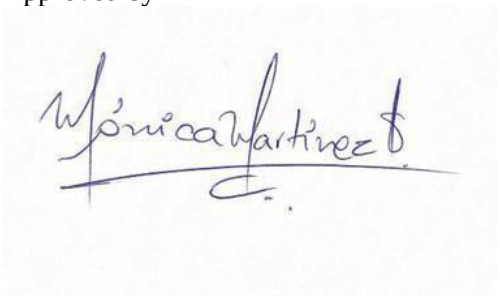
ABSTRACT:

The right to privacy and data protection in Ecuador's financial sector is fundamental, especially where regulations on personal data interact with constitutional rights. This research examines the management of credit and personal information by financial institutions, focusing on debt collection procedures, where banking secrecy is crucial to preserving trust within the user-entity relationship. Financial institutions are not primarily responsible for managing personal data. Instead, third-party agents involved in debt recovery frequently misuse this information, leading to inadequate protection. The Constitution of the Republic of Ecuador, the Organic Monetary and Financial Code, and the Organic Law on Data Protection emphasize transparency, confidentiality, and legality as essential principles in handling financial users' data. This research also examines adhesion contracts, which are prevalent in the financial sector and set terms without allowing negotiation. These contracts, despite their non-negotiable nature, are legally required to respect consumer rights and provide a degree of fairness to users. Furthermore, the study underscores the importance of implementing robust privacy policies and promoting a comprehensive legal framework that limits unauthorized access to sensitive financial data and aligns with international norms. Finally, a comparative analysis of international standards in financial data protection highlights approaches that balance data security and the right to privacy, providing insights into best practices and potential regulatory enhancements. This analysis seeks to enhance understanding of ways to strengthen privacy and data protection regulations within Ecuador's financial sector, ensuring better safeguards against the misuse of user data.

Keywords: Adhesion contracts, Confidentiality, Data protection, Financial entities, Privacy

Lucía Abdo
0958641459
lucia26@es.uazuay.edu.ec

Approved by



Lcda. Mónica Martínez Sojos, Mgt.
Cod. 29598

ÍNDICE

INTRODUCCIÓN

La gestión de datos personales ha cobrado importancia, especialmente en el ámbito financiero, donde la privacidad y el manejo adecuado de la información son esenciales para proteger los derechos de los usuarios. Así, es importante determinar la responsabilidad que tienen las entidades bancarias en la gestión de datos personales, explorando como el incumplimiento en la protección de estos datos puede vulnerar la privacidad de los deudores. De esta forma, se examinará el marco normativo que regula la protección de datos personales en el Ecuador, incluyendo tanto la Constitución como la Ley Orgánica de Protección de Datos Personales y su aplicación en las actividades bancarias, enfocándose en las prácticas y procedimientos para el cobro de obligaciones.

Además, se analizarán conceptos claves como el derecho a la privacidad y la expectativa razonable de privacidad, desglosando los principios y regulaciones que protegen la información personal en un contexto financiero. Así, se exploran los tipos de datos sensibles que manejan las entidades financieras y las implicaciones legales de su mal manejo.

En este contexto, es importante agregar un análisis comparativo con legislaciones internacionales, en concreto con la normativa de protección de datos de la Unión Europea y con la de España, con el fin de contrastar las regulaciones ecuatorianas y proponer mejoras que fortalezcan la privacidad del deudor en el ámbito bancario.

Finalmente, este estudio presenta entrevistas con usuarios financieros y con representantes de la Superintendencia de Bancos, proporcionando perspectivas prácticas sobre el impacto de las prácticas de privacidad y confidencialidad en la confianza del usuario hacia el sistema financiero. Con ello, se pretende aportar una visión integral sobre los desafíos y responsabilidades que enfrentan las entidades bancarias en el manejo de datos personales y proponer recomendaciones para asegurar una gestión ética y legalmente adecuada de la información de los deudores.

CAPÍTULO 1
1.1 DERECHO A LA PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

1.1.1 DERECHO A LA PRIVACIDAD

El derecho a la privacidad es un pilar fundamental en la protección de la dignidad y autonomía individual. Este derecho busca salvaguardar la esfera personal y confidencial de los individuos, garantizando que su vida privada no sea vulnerada, protegiendo así la información personal y sensible. El respeto a la privacidad es esencial para el ejercicio pleno de otros derechos fundamentales. De esta forma, en un mundo cada vez más interconectado y digitalizado, la protección de la privacidad se ha vuelto esencial.

En este contexto, para comprender este derecho, es fundamental comenzar con su definición, por ello, se debe partir de una concepción general. La Real Academia de la Lengua Española define a la privacidad como el derecho a la protección de la vida privada que abarca aquellos aspectos de la vida personal que deben resguardarse de cualquier tipo de intromisión. (Real Academia Española, 2023).En este sentido, la base de la privacidad radica en la protección del individuo, garantizando que la información personal sea utilizada únicamente con su consentimiento expreso, asegurando que el control sobre la divulgación y el uso de dicha información permanezca en manos del propio titular. Siendo importante, por un lado, que la persona dé su consentimiento para el acceso a su información, así también como oponerse a que la misma sea divulgada (Pfeiffer, 2008).

En este sentido, la parte medular del derecho a la privacidad es la voluntad del individuo, misma que radica en la decisión sobre qué información puede ser utilizada de manera pública, estableciendo su alcance y uso de esta. Así, para el autor Sanz la privacidad es una característica esencial de la naturaleza humana (Sanz, 2018). Esto quiere decir que la privacidad para el ser humano tiene un componente primordial cuando se trata del desarrollo y bienestar de cada individuo. Dentro del derecho a la privacidad se encuentran tres elementos fundamentales, la soledad, el anonimato y el secreto. Siendo un estado que al no tener carácter absoluto, puede ser revocado por el titular de la información cuando así lo decida.

Con todo lo analizado cabe agregar además lo establecido por el filósofo Locke, quien le da un sentido de propiedad a este derecho, estableciendo que el derecho a la

privacidad depende del derecho de propiedad, el cual solo le corresponde al dueño (Vergés,2022). De esta manera, se puede deducir que, además, el derecho a la privacidad tiene un carácter restringido, es decir, el uso de la información queda bajo el control del titular.

1.1.2 EXPECTATIVA RAZONABLE DE PRIVACIDAD

La expectativa razonable de privacidad es un concepto fundamental en la protección de los derechos individuales, especialmente en el ámbito de la protección de datos personales. Este concepto surge principalmente del desarrollo jurisprudencial llevado a cabo por la Corte Suprema de los Estados Unidos, quienes otorgan un aporte fundamental en la formulación y expansión del derecho a la privacidad y a la intimidad.

Así, dentro de este ámbito jurisprudencial, este concepto se desarrolló en el marco penal, donde el punto fundamental de la investigación se dio por el delito de apuestas ilícitas. Para entender este caso, la parte esencial fue la recepción de una llamada realizada por el procesado desde una cabina pública. Esta intervención desató una serie de discusiones basándose en las actuaciones que puede realizar fiscalía; entendiéndose que la misma actuó sin orden judicial previa para realizar este tipo de acciones. La Corte Suprema de los Estados Unidos de América llegó a la conclusión de que el accionante tenía una expectativa razonable de la privacidad y por ello, su derecho a la intimidad se vio afectado, siendo que este tipo de actuaciones pueden realizarse únicamente mediante orden judicial. A raíz de esto se concluyó que esta idea se refiere al nivel de protección de la intimidad que una persona puede esperar razonablemente frente a posibles interferencias tanto del Estado como de la sociedad en general, ya sea en el ámbito penal o civil (Corte Constitucional del Ecuador, 2021).

La expectativa razonable de privacidad establece el nivel de protección que una persona puede esperar frente a posibles injerencias del Estado y de la sociedad. Este concepto abarca tanto el ámbito penal, en el que regula la obtención de pruebas y la intervención estatal, como el ámbito civil, en el que protege el derecho a la intimidad y regula el manejo de información personal. Este marco de protección busca equilibrar la privacidad individual con las necesidades de seguridad y el interés público.

En este contexto, la Corte Constitucional de Colombia en la sentencia número C-881/14, realiza su propio análisis de este tema, y establece que se necesitan dos requisitos sobre los cuales se basa la expectativa razonable de privacidad; los cuales son:

a. **Expectativa subjetiva actual de privacidad**: desglosando esta idea podemos encontrar que este componente se refiere a la percepción personal del individuo sobre su derecho a la privacidad en un contexto específico. Es decir, si una persona siente que tiene derecho a mantener cierta información o actividades en privado, esa percepción es la base de su expectativa subjetiva.

   Su importancia recae en entender cómo una persona valora su privacidad en un momento dado. Esto puede variar según la situación, el lugar, o el tipo de información en cuestión. Por ejemplo, una persona puede esperar privacidad en sus comunicaciones personales, pero no en sus interacciones públicas.

b. **La sociedad puede asumir esta expectativa como razonable:** Este componente implica que la expectativa subjetiva de privacidad debe ser también considerada razonable por la sociedad en general. Es decir, la percepción individual de privacidad debe alinearse con las normas y valores sociales sobre lo que se considera un ámbito razonable de privacidad.

   La importancia recae en que la aceptación social es crucial para establecer una norma legalmente protegida, asegurando de esta forma que las expectativas de privacidad individuales no solo sean reconocidas, sino también respaldadas por las normas sociales y legales.

Analizando esto, la misma Corte Constitucional de Colombia en su sentencia número T-547/17 (Corte Constitucional de Colombia, 2017) , define que la expectativa de privacidad es un factor clave para determinar si ciertos aspectos de la vida personal están protegidos por el derecho a la intimidad o si, en cambio, pueden ser divulgados o interferidos por terceros.

De esta forma, se puede llegar a concluir que existe dos tipos de elementos que concurren para establecer la expectativa razonable de privacidad. Por un lado, está el elemento subjetivo, que se fundamenta en la percepción de quien siente que su intimidad ha sido vulnerada, estableciendo que la esfera afectada está protegida contra cualquier tipo de injerencia, y, por otro lado, el elemento objetivo implica que la sociedad considere

esa expectativa como razonable, es decir, que se pueda determinar que es válida y puede ser defendida frente a terceros.

La Corte Constitucional del Ecuador hace una reflexión al respecto, donde establece que la existencia de estos elementos depende de factores tanto objetivos como subjetivos, los cuales deben ser considerados en el análisis de cada caso particular para establecer si realmente existe una expectativa de privacidad. (Corte Constitucional del Ecuador, 2021). Así pues, se debe analizar las circunstancias dadas en cada caso, tomando en cuenta que tipo de información se discute, la autorización de la persona, la relación que tiene el titular de los datos y quien se encarga del tratamiento, para poder establecer, si efectivamente se está frente a un caso de intromisión a la vida privada.

1.1.3 DERECHO A LA INTIMIDAD DENTRO DE LA CONSTITUCIÓN

Por otro lado, tenemos el derecho a la intimidad, mismo que se encuentra recogido en la Constitución de la República del Ecuador. En este sentido, se debe resaltar que la misma abarca más allá de la esfera personal que usualmente se asocia con la intimidad, conteniendo así los ámbitos sociales, políticos y económicos que los seres humanos crean y desarrollan a lo largo de su vida.

En este contexto, es necesario realizar una definición sobre el mencionado derecho a la intimidad. Según el tratadista Torre , quien da una concepción amplia y concreta sobre este derecho, establece que el derecho a la intimidad está asociad o con el ámbito más privado de los individuos (Torre, 2015), implicando que tanto el estado como la sociedad tienen el deber de respetar y salvaguardar ese espacio personal de privacidad.

Se entiende así que el estado es el responsable de garantizar y proteger el derecho a la intimidad, esto mediante la formulación y aplicación de normas jurídicas, mismas que cumplen con el objetivo de salvaguardar este derecho; evitando así la intromisión arbitraria en los aspectos reservados de los individuos.

De esta forma, el derecho a la intimidad está contenido en la Constitución de 2008 de la República del Ecuador. Dentro del artículo 66 numeral 20[1], se establece la protección del ámbito personal, salvaguardando aquellos aspectos de la vida privada que

[1] Art. 66.- Se reconoce y garantizará a las personas: 20. El derecho a la intimidad personal y familiar. (Constitución de la República del Ecuador, 2008).

no deben ser divulgados sin el consentimiento explícito del individuo. Como es el caso del ámbito familiar que hace referencia a la protección de la privacidad dentro del núcleo familiar ;implicando que las relaciones entre sus miembros y las actividades cotidianas realizadas en el ámbito del hogar sean protegidas de interferencias externas.

En lo principal, el derecho a la intimidad en el ámbito personal incluye esencialmente la correspondencia, comunicaciones y cualquier otra información que forme parte de la esfera privada de los individuos. Conteniendo de esta forma un marco jurídico que garantiza y protege el derecho que es otorgado a los mismos, para que sean ellos quienes decidan negar o excluir a terceros de conocer ciertos aspectos de su vida. Pero ¿Qué significa que el derecho a la intimidad sea fundamental? Para poder responder esta pregunta es necesario establecer que la Constitución de la República del Ecuador tiene una característica fundamental, siendo considerada como *garantista.* Esto se debe a que incluye una amplia variedad de derechos que deben ser aplicados de manera inmediata y directa. Relacionando a los derechos fundamentales como esa conexión con los valores esenciales que los individuos tienen, siendo estos la libertad, igualdad y la dignidad.

Dichos valores otorgan a cada uno de los individuos una autonomía, que en el derecho según como lo establece el Doctor Jorge Zavala, este concepto de persona se basa en atributos como la voluntad, el raciocinio y el conocimiento, que en conjunto la constituyen como un individuo autónomo (Zavala Egas, 2019).Sin embargo, este postulado trasciende el ámbito meramente jurídico, dado que las constituciones, en términos generales, se estructuran en función de las personas; la construcción de la constitución se centra en proteger a las personas de actuaciones que se realicen sin su consentimiento o, incluso, en contra de su voluntad.

Así pues, el derecho a la intimidad al ser fundamental tiene una interdependencia con la personalidad, siendo este un derecho innato que nace con la persona. Lo cual significa que para ejercer este derecho no se necesita un acto jurídico para adquirirlo, pues de manera inmediata el titular ostenta la potestad para proteger todo lo inherente a su persona.

Complementando esta idea, el tratadista Olivares aporta una clara y precisa definición del derecho a la intimidad; donde establece que el mismo se deriva de la

capacidad de cada individuo para decidir por sí mismo cómo, cuándo y qué cantidad de su información personal puede ser compartida con otros, considerando previamente si esa divulgación pudiera causarle algún perjuicio moral o patrimonial. (Olivares, 2000). Teniendo así otro enfoque al de la Constitución de la República del Ecuador. Debido a que, en ella se da protección del estado hacia las personas, evitando así intromisiones arbitrarias del mismo y de la sociedad en general. Sin embargo, Olivares da una visión desde la persona a quien le pertenece la información, siendo esta quién debe abstenerse de divulgar la información que considere que pueda ser perjudicial en las distintas esferas de su vida.

Ambos puntos de vista están interconectados, ya que se debe considerar que, aunque la persona es responsable de limitar qué información sobre su vida puede ser divulgada, ya sea a nivel familiar, económico, social o incluso político, el avance tecnológico ha llevado a una mayor interconexión entre individuos. Como resultado, las intromisiones son cada vez más comunes.

1.1.4 PRINCIPIOS INHERENTES AL DERECHO A LA INTIMIDAD

El derecho a la intimidad es un derecho fundamental que no solo está plasmado en la Constitución de la República del Ecuador; sino que además es recogido en tratados internacionales, como lo es la Declaración de Derechos Humanos del año 1948 donde se manifiesta que ninguna persona deberá ser sometida a intervenciones arbitrarias en su vida privada, familia, domicilio o correspondencia, ni a ataques contra su honor o reputación (Declaración Universal de los Derechos Humanos, 1948). De esta forma, es importante establecer primero los principios en que dicho derecho se sustenta para conocer cuando se está ante injerencias arbitrarias.

Así pues, la Corte Constitucional de Colombia es clara cuando define cinco principios que son desarrollados dentro de la sentencia C-640/10. De esta manera, el primer principio es de LIBERTAD, siendo el más fundamental, debido a que es la persona titular de la información quien tiene la potestad de escoger que puede ser divulgados o bien registrados, pero siempre que el consentimiento del titular sea libre, previo, expreso o tácito, salvo que la legislación le obligue a divulgar dicha información. (Corte Constitucional de Colombia, 2010). Entendiéndose que las personas tienen una suerte de soberanía al momento de revelar su información privada.

Sin embargo, es necesario tomar en cuenta una circunstancia que debe ser analizada. Si bien las personas tienen el derecho a escoger que información de su vida privada puede revelarse y divulgarse, hay una limitación a dicha libertad que la Constitución de la República del Ecuador la prevé, siendo el caso de la información es requerida judicialmente.

Para entender esto, un claro ejemplo es la información financiera. Pues bien, estos datos no pueden ser divulgados de forma libre por las entidades bancarias, sin embargo, en un juicio por pensiones alimenticias ,donde el alimentante tiene obligaciones por cumplir, se puede llegar a tener la información sobre cuánto dinero tiene, por ejemplo, en cuentas bancarias. Esta información puede ser exhibida mediante una orden judicial la cual va dirigida al máximo órgano de control de bancos que en el caso ecuatoriano viene a ser la Superintendencia de Bancos. Mediante una autorización previa de este órgano, se puede llegar a revelar la información bancaria de las cuentas.

Como segundo y tercer principio están la finalidad y necesidad, mismos que van estrechamente ligados. En el primero se establece que la información personal debe ser recolectada con un propósito específico y legítimo, siendo utilizada para un fin concreto, y, el segundo, que solo debe recolectarse y utilizarse la información personal que sea estrictamente necesaria para cumplir con un objetivo, enfocado en limitar la cantidad de datos recolectados. El cuarto principio, trata de la Veracidad, se establece que, una vez la información ha sido divulgada, esta debe pertenecer a hechos reales, prohibiendo así la divulgación de datos erróneos o falsos.

El principio de integridad establece que, una vez obtenidos los datos, estos no deben divulgarse de manera parcial, fraccionada o incompleta. Este principio subraya que la información personal divulgada debe ser proporcionada en su totalidad, sin omitir detalles relevantes que puedan alterar su correcta comprensión o interpretación.

1.1.5 DERECHO A LA INTIMIDAD VS DERECHO A LA PRIVACIDAD

En el ámbito jurídico, es común encontrar cierta confusión en cuanto los conceptos de derecho a la intimidad y derecho a la privacidad, llegando incluso a utilizarlos como

sinónimos. Sin embargo, aunque ambos derechos están intrínsecamente relacionados y buscan proteger aspectos fundamentales de la vida de las personas, no son equivalentes.

Por un lado, cuando se hace referencia al derecho a la intimidad, y, como lo describe la Constitución de la República del Ecuador, se abarca aspectos de la conducta social de las personas, donde se involucra aspectos de su vida, bien sean personales o familiares. Este derecho como ya se mencionó antes está reconocido en la constitución, entendiéndose que es importante considerar a la intimidad un bien jurídico protegido y, además, un derecho fundamental, cuenta con un nivel de protección específico y complementario con el derecho a la privacidad. (Tiguerro, 2021).

Por otro lado, el derecho a la privacidad según Vergés establece que se necesita de la exposición pública de su titular para poder ser ejercido. (Vergés, 2022).En este sentido, para que el derecho a la privacidad sea efectivo, debe haber algún nivel de interacción o presencia del individuo en el ámbito público. Esto implica que el derecho a la privacidad se activa o se vuelve relevante en situaciones donde los datos o la información personal del individuo son susceptibles de ser observados, recopilados o utilizados por otros, destacando la importancia del control sobre cómo y cuándo se divulga dicha información.

Sin embargo, para que se de este nivel de interacción dentro de la sociedad, el derecho a la privacidad implica la voluntad de la persona para que se conozcan ciertos aspectos personales de su vida. Esto tiene relación según lo que establece Vergés, donde el derecho a la privacidad está condicionado por el derecho a la propiedad, ya que solo el propietario tiene el control exclusivo sobre ella (Vergés, 2022, pág. 92). Teniendo en cuenta lo establecido con anterioridad, hay aspectos personales de los individuos que pueden ser recolectados, difundidos y almacenados, siempre y cuando el dueño de esa información mediante su voluntad haya decidido que estos sean difundidos.

De esta forma, para entender de manera precisa la diferencia entre la intimidad y la privacidad, se debe hacer referencia al siguiente silogismo, los asuntos íntimos son privados, pero no todos los asuntos privados pueden considerarse íntimos. (Tiguero, 2021). En resumen, cuando el derecho a la intimidad se ve vulnerado en situaciones muy concretas de la vida, esto a su vez acarrea la vulneración a la privacidad, sin embargo, si

se da una vulneración al derecho a la privacidad no necesariamente se vulnera la intimidad del individuo.

Por ejemplo, cuando una persona negocia la compra de una propiedad, la negociación es un asunto privado porque involucra detalles financieros y contractuales que no son de conocimiento público, sin embargo, esto no es un asunto íntimo ya que no toca aspectos profundamente personales o sensibles del individuo.

Sin embargo, el estado de salud de un individuo es un asunto íntimo, ya que involucra información muy personal y sensible que generalmente solo se comparte con familiares cercanos y profesionales de la salud. Este tipo de información, además de ser privada, tiene un carácter íntimo debido a su naturaleza.

Resumiendo, El derecho a la intimidad se refiere, en términos generales, a la protección de la vida privada y familiar buscando resguardar aspectos personales y sensibles de la intrusión indebida, y, por otro lado, el derecho a la privacidad tiene un espectro más amplio, abarcando no solo la protección de la información personal, sino también el control sobre el uso y la difusión de datos personales en diversos contextos.

1.2. DATOS PERSONALES DEFINICIÓN

Este acápite se centrará en desglosar y entender el concepto de datos personales, abordando sus diferentes componentes y características esenciales. A través, del análisis de definiciones legales y doctrinales, se busca una comprensión profunda y precisa de este concepto. Este análisis es fundamental para comprender cómo se maneja y protege la información personal en la actualidad.

De esta forma, se debe empezar por la definición más básica, entendiendo sé que dato es la conformación ordenada de ceros y unos, que según la informática estos pueden ser manipulados mediante operaciones matemáticas. Con esto, se debe entender que el tratamiento de datos a lo largo del tiempo no solo ha sido materia de estudio del derecho, ya que los datos per se son encontrados en todos los aspectos de nuestra vida.

Pensemos así, en la esfera militar, el manejo y análisis de datos es crucial para el éxito de diversas operaciones, especialmente en el ámbito del espionaje y la seguridad nacional. Un claro ejemplo de esto radica en la capacidad de descifrar claves o mensajes encriptados, siendo una actividad esencial para la inteligencia militar. Pero también, se encuentran en aspectos cotidianos dela vida, por ejemplo, las decisiones basadas en datos

se han convertido en una herramienta esencial en diversas disciplinas y sectores. Tal es el caso de las empresas donde utilizan complejas fórmulas al momento de realizar sus productos para optimizar la atención del cliente, mejorar la eficiencia operativa y aumentar la satisfacción del usuario.

Por otro lado, se tiene una definición más específica, situándose en la raíz etimológica de la palabra Dato. La misma proviene del latín *DATUM* que lleva como significado *lo que se da o lo dado.* Este término ha evolucionado a lo largo del tiempo para referirse a cualquier pieza de información que puede ser utilizada para análisis, toma de decisiones o como base de conocimiento.

Esta definición se puede complementar con lo señalado en la Real Academia de la Lengua Española, donde se establece que dato es la información específica que permite su comprensión precisa o que facilita la deducción de las consecuencias derivadas de un hecho (Real Academia Española, 2023).Esta definición resalta la importancia de los datos como elementos clave para comprender y analizar la realidad, así como para prever y evaluar las posibles implicaciones de ciertos eventos o acciones. En este sentido, para el catedrático Rubén Flores, quien tiene una visión general de dato establece que un dato personal incluye información como el nombre, sexo, nacionalidad, domicilio, estado civil, número de afiliado a la seguridad social, entre otros. (Flores, 2007).

Sin embargo, en el contexto actual, especialmente en el ámbito legal y tecnológico, el término "dato" ha adquirido una relevancia particular, ya que abarca una amplia gama de información personal que, al ser recopilada, procesada y almacenada, puede tener implicaciones significativas para la intimidad y los derechos individuales. Por lo tanto, en la actualidad establecer que datos personales hace referencia únicamente a nombres, direcciones, estado civil etc, viene a ser limitado.

De esta forma, para tener una definición más clara de datos personales, se debe recurrir a la Sentencia No. 2064-14-EP/21 emitida por la Corte Constitucional del Ecuador, siendo una decisión judicial relevante que aborda aspectos críticos del derecho a la privacidad y la protección de datos personales en Ecuador. En particular, dentro de este fallo se analiza la protección que deben recibir los datos personales frente a su recolección y procesamiento; tanto de entidades públicas como privadas, garantizando que se respeten los derechos fundamentales de las personas.

La Corte sostiene que los datos personales e información sobre una persona, tal como están definidos en la Constitución y siguiendo el principio pro homine, deben entenderse de manera amplia. Esto implica que cualquier información que se relacione,

directa o indirectamente, con una persona o sus bienes, en cualquiera de sus aspectos o dimensiones, puede considerarse como un dato personal. Dicha información puede ser solicitada mediante el ejercicio del derecho de hábeas data. Así, es suficiente que la información, independientemente de cómo se presente, haga referencia a algún aspecto de la persona, ya sea objetivo o subjetivo, o que guarde relación con ella según su contenido, finalidad o resultado, para ser considerada un dato personal (Corte Constitucional del Ecuador, 2021).

Esta definición es precisa en cuanto a datos personales. Como se analizó con anterioridad, se establecía que cuando se hacía referencia a los mismos se limitaba al nombre, estado civil etc. Sin embargo, la Corte constitucional del Ecuador amplía esta definición y hace alusión a que los datos personales enmarcan cualquier tipo de información que de una referencia tanto de la persona como de sus bienes. Abarcando así una esfera amplia de lo que conocemos como datos personales.

Para sustentar está definición, la Corte Constitucional hace referencia a lo que establece el Consejo Europeo de Protección de Datos, la cual implementa que cualquier dato referente a una persona natural identificada o que pueda ser identificada («el titular»); se entenderá por persona natural identificable a toda aquella cuya identidad se pueda establecer, ya sea de manera directa o indirecta, especialmente a través de un identificador como un nombre, un número de identificación, información de ubicación, un identificador en línea o varios elementos que correspondan a su identidad física, fisiológica, genética, psicológica, económica, cultural o social (Consejo Europeo de Protección de Datos de la Unión Europea, S.F).

Para entender lo establecido por la CEPD, se debe hacer un desglose de las partes importantes de esta definición. Como primero, tiene que haber un interesado, quien es el sujeto al que pertenece la información , es decir el titular. En este caso tiene que ser bien una persona identificada, esto significa que se sabe con exactitud quien es el individuo al cual se está haciendo referencia o bien una persona identificable, cuando se menciona este último ,quiere decir que no se sabe con exactitud la identidad de la persona , sin embargo, cubre situaciones donde la identidad puede ser determinada directa o indirectamente, a partir de la información que se tenga disponible. Pero ¿Cómo se identifica a esta persona?, como segundo elemento está el medio identificador, lo que se considera como el nombre, número de identificación etc. y a su vez, un individuo puede ser identificado mediante elementos de identidad física, cultural o social.

De esta forma, se puede consolidar estas definiciones y establecer que datos personales no sé queda en la esfera del nombre, cédula, estado civil etc. sino que más bien es todo aquello que haga referencia a una persona o sus bienes, sea esta identificada o identificable mediante información que haga referencia a su identidad física, cultural o social.

1.2.1 PROTECCIÓN DE DATOS PERSONALES

La protección de datos personales se ha convertido en un tema de crucial importancia. Los avances tecnológicos han facilitado la recopilación, almacenamiento y procesamiento de grandes volúmenes de información personal, lo cual plantea d desafíos significativos en cuanto a la privacidad y la seguridad de los individuos. La protección de datos personales no solo es un derecho fundamental reconocido en diversas legislaciones nacionales e internacionales. Tal es el caso de la Constitución de la República del Ecuador, en la cual reconoce en su artículo 66 numeral 19[2], el derecho a la protección de datos personales, principalmente el uso, acceso y la decisión que el titular de estos tiene respecto a terceras personas.

Aunque la Constitución establece los lineamientos generales para los derechos, es necesario un desarrollo más amplio para garantizar su protección y cumplimiento efectivo. En este contexto, en el año 2021 se promulgó la Ley Orgánica de Protección de Datos Personales, cuyo principal objetivo es asegurar el ejercicio del derecho a la protección a los mismos. Como se señaló anteriormente, este derecho abarca tanto el acceso como la capacidad de decisión sobre la información personal, con el fin de brindar una protección integral.

Para analizar de manera profunda se debe hacer un desglose de este artículo 19 y complementarlo con lo que establece la Ley Orgánica de Protección de Datos. De esta forma, encontramos en la Constitución cuatro principales situaciones cuando se da la protección de datos personales. La primera se trata sobre el acceso y decisión sobre la información y datos personales, este aspecto implica que las personas son quienes tienen el control sobre qué información puede llegar a divulgarse, esto quiere decir que se les otorga el derecho a que una vez que esta información personal sea conocida, los individuos tengan acceso a la misma, además deben conocer cómo y para qué son

[2] Art. 66.- Se reconoce y garantizará a las personas:
19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Constitución de la República del Ecuador, 2008).

utilizados sus datos personales y decidir si se autoriza o no el uso de estos. Siendo este control algo fundamental como medio de protección de la privacidad ,y, así evitando que la información que se autorizó para conocimiento público no sea utilizada de forma indebida.

Como segundo punto está la protección, esto abarca un espectro más amplio que solo evitar el uso indebido de los datos personales. Además, se requiere de medidas de seguridad que garanticen la integridad y la confidencialidad de la información. Esto incluye la adopción de tecnologías de seguridad, política de protección de datos, capacitación del personal que maneja dicha información y, como garantía para su protección , un órgano encargado de velar el cumplimiento de protección de datos.

El tercer punto de este análisis se centra en la recolección, archivo, procesamiento, distribución o difusión de datos. Cada una de estas etapas debe realizarse bajo ocho principios contenidos en la Ley Orgánica de Protección de datos, siendo el primero de juridicidad. El cual establece que los datos personales deben ser tratados con apego estricto y cumplimiento de derechos, principios y obligaciones que están contenidas en la Constitución de la República del Ecuador, así como el cumplimiento de lo establecido en tratados internacionales.

El segundo principio trata de lealtad. La Ley Orgánica de Protección de Datos Personales en cuanto a este principio establece que el manejo delos datos personales debe ser transparente, por lo que los titulares deben ser informados de manera clara sobre la recolección, uso, consulta o cualquier otro tipo de tratamiento de sus datos, así como sobre las formas en que estos serán o pueden ser procesados (Ley Orgánica De Protección De Datos Personales, 2021).Siendo así, el titular de los datos personales siempre debe estar al tanto de cómo y para qué sus datos van hacer utilizados, prohibiendo así que los datos personales sean manejados para fines ilícitos.

El tercer principio se fundamenta en la transparencia, estableciendo que, una vez obtenidos los datos personales, su titular debe ser debidamente informado sobre el tratamiento que recibirán. Además, se debe garantizar que, tras su recolección, los datos sean fácilmente accesibles para su titular.

Como cuarto principio está la finalidad. En el cual se debe tomar en cuenta dos principales consideraciones. La primera es que los datos personales pueden ser utilizados únicamente para el fin que son recolectados. En este sentido, la Organización de los Estados Americanos hace alusión a la forma que los datos personales deben ser tratados, dando así 8 parámetros en los cuales el tratamiento de datos tiene una finalidad específica:

a. Primer parámetro, se basa fundamentalmente en la voluntad, que debe otorgar el titular de los datos personales, dicha voluntad tiene que ser expresa e informada ya sea para uno o varios fines para los cuales los datos van a ser tratados.

b. Segundo parámetro, aborda la necesidad del tratamiento, es decir, cuando estos sean necesarios para que se cumpla un fin en concreto.

c. Tercer parámetro, se refiere a situaciones en las que el tratamiento de los datos personales es esencial para que, bien sea una entidad o una persona natural pueda cumplir con una obligación que el titular de los datos ha aceptado.

d. Cuarto parámetro, se sustenta en que el tratamiento de datos es necesario para proteger intereses vitales, bien sean del titular de la información o de un tercero.

e. Quinto parámetro, se basa netamente en un tratamiento de datos personales en el ámbito público, es decir, para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable de Datos (Organización de Estados Americanos, 2022). Esto significa que los datos pueden ser tratados sin el consentimiento explícito del titular si el tratamiento es esencial para llevar a cabo tareas o funciones que beneficien al público o que sean parte de las competencias legales de una entidad pública.

f. Sexto parámetro, hace referencia a que el tratamiento de datos sea necesario para satisfacer intereses legítimos del responsable de los datos. Es decir, se refiere a los objetivos o finalidades que el responsable del tratamiento de los datos (como una empresa o una organización) tiene, y que son considerados válidos y razonables dentro de un marco legal y ético.

g. Séptimo parámetro, deja a un lado la voluntad del titular de los derechos para realizar el tratamiento de los datos cuando de por medio está el cumplimiento de una orden judicial; siempre y cuando esté debidamente motivada y sea expedida por la autoridad competente.

h. Octavo parámetro, cuando el tratamiento de datos sea necesario para reconocimiento o defensa de los derechos del titular ante una autoridad.

Los datos personales deben ser tratados siempre dentro del marco legal y con un fin legítimo. Esto puede ser con el consentimiento del titular de la información o para

cumplir con un interés público, pero en todos los casos, es esencial que no se vulneren los derechos del titular.

Sin embargo, la Ley Orgánica de Protección De Datos Personales en su artículo 10 literal D[3], da la posibilidad que los datos personales recogidos puedan tener un tratamiento distinto para el cual inicialmente fueron recolectados. Siempre y cuando estos sean compatibles con los fines iniciales. Esto protege al titular de los datos de usos inesperados o no deseados de su información personal.

Para determinar esta compatibilidad, se deben considerar varios factores, incluyendo el contexto de la recolección de los datos, la información proporcionada al titular, sus expectativas razonables, la naturaleza de los datos, las posibles consecuencias para los titulares, y la existencia de garantías adecuadas. Esto asegura que el uso de los datos sea transparente, justificado, y seguro, protegiendo siempre los derechos del titular. Como quinto principio, se basa en la pertinencia y minimización de datos personales. Este principio tiene mucho que ver con el principio de finalidad, ya que la información otorgada por el titular debe ser estrictamente utilizada para el fin el cual se pactó. Esto tiene que ver con la expectativa razonable mencionada con anterioridad, esto significa que se debe tener en cuenta la confianza que tiene el titular, basada en su relación con el responsable del tratamiento.

Un claro ejemplo de esto es, cuando un cliente proporciona sus datos a una empresa para la compra de un producto, es razonable que espere que sus datos puedan ser utilizados para gestionar la entrega y el servicio postventa, pero no para fines totalmente ajenos como publicidad de terceros.

El sexto principio se basa en la proporcionalidad del tratamiento. Con esto se entiende que el tratamiento que se da a los datos debe ser apropiado para alcanzar las finalidades para las cuales se recogieron. Esto implica que el método de tratamiento debe ser adecuado, y, para cumplir con el propósito específico establecido, evitando la

[3] Art. 10.- Principios.- Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de: d) Finalidad.- Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular: no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta Ley. El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista. (Ley Orgánica De Protección De Datos Personales, 2021).

recopilación y el uso de datos en exceso, recolectando únicamente información necesaria y puntual, de esta forma, se protege el derecho del titular de los datos personales.

El séptimo principio es la confidencialidad, cuyo fundamento se basa en el sigilo y la reserva que deben observar los responsables del tratamiento de los datos personales. En este sentido, los datos no deben ser procesados ni divulgados con fines distintos a los que motivaron su recolección. De esta manera, el tratamiento de los datos debe limitarse exclusivamente a los objetivos específicos para los cuales fueron recabados, garantizando así que la información no se utilice con propósitos diferentes a los previamente informados al titular.

Y como ultimo principio, se trata de la calidad y exactitud de los datos personales, entendiéndose que los datos deben ser correctos y reflejar la realidad con precisión, además estos tienen que estar completos, evitando la omisión de alguna de sus partes, estos no deben ser ambiguos y la información debe poder ser verificada para asegurar su veracidad; para esto los datos deben estar al día, reflejando la información más reciente y relevante para los fines del tratamiento.

Dentro de este principio, se debe establecer que además de calidad y exactitud de los datos, se debe tener medidas de corrección, que pueden a su vez dar la posibilidad de suprimir o rectificar la información otorgada. De esta manera, en el caso de que los datos sean inexactos o que ya no sean necesarios para los fines para los cuales se tratan, se deben implementar medidas para corregir o eliminar los datos personales.

Como último punto, está la autorización del titular o mandato de la ley. De esta manera, ninguna entidad puede realizar el proceso antes mencionado sin el consentimiento expreso, libre e informado de la persona a quien pertenece los datos personales. Con este último apartado, se debe entender que la persona dueña de los datos personales debe estar en plena conciencia del cómo y para que ,sus datos son recolectados y, además conocer los derechos que tiene con relación a estos. Sin embargo, la norma también otorga la posibilidad de tener acceso a los datos de las personas por mandato de ley.

Esta situación puede darse por ejemplo, con la Superintendencia de Bancos del Ecuador, al estar encargada de todo lo referente al control y supervisión de las entidades del sector tanto público como privado del sistema financiero y además del sistema nacional de seguridad social. De esta forma, cuando una persona está en un juicio de cobro de una obligación, la misma puede solicitar mediante la función judicial que se oficie a la Superintendencia de Bancos para que este disponga al sistema financiero la

respectiva información sobre cuentas de ahorro, corrientes e inversiones con la finalidad de saber cuál es la situación financiera de una persona. En este caso, no se necesita el consentimiento del titular para acceder a esta información sino meramente por el mandato de la ley.

En este contexto, una vez explicada la función de los datos personales, se debe entender el alcance de la protección de datos. Así pues, la Corte Constitucional del Ecuador, en la sentencia número 2064-14-EP/21 establece que es importante señalar que la protección de un dato personal no depende del formato en el que se encuentre (Corte Constitucional del Ecuador, 2021). En otras palabras, ya sea que el dato esté registrado en un soporte físico o almacenado en formato digital, el nivel de protección debe ser equivalente en ambos casos.

Entendiéndose que, en la actualidad, con el avance cada vez más amplio de la tecnología, ha cambiado la precepción sobre los datos personales, al dar la posibilidad de que estos pueden ser encontrados en cualquier tipo de medio; bien sea físico o tecnológico, sin embargo, todos tienen la misma protección ante la ley. Siendo esto crucial para garantizar la seguridad y privacidad de la información personal, sin importar si está almacenada en medios físicos o digitales.

Pues los datos personales pueden estar contenidos en medios físicos tales como formularios, expedientes y cualquier otra forma tangible de almacenamiento de información. La protección en estos casos implica medidas como el almacenamiento seguro de documentos, el control de acceso físico a los archivos. Por otro lado, están los medios digitales, teniendo estas una gama más amplia de formatos en cuanto a datos. Mismos que son desde bases de datos electrónicos, archivos en la nube, correos electrónicos y más. La protección en estos casos requiere medidas técnicas y organizativas específicas, como el uso de encriptación, sistemas de autenticación y autorización, copias de seguridad, y ciberseguridad.

De esta manera, se puede concluir que la protección a los datos personales está contenida como derecho en la Constitución de la República del Ecuador y que además, se tiene una norma especializada para su cumplimiento. Entendiéndose que el alcance que se da a la protección de datos personales se da tanto en medios físicos como digitales, puesto que en la actualidad con el avance de la tecnología los datos personales pueden ser encontrados en cualquier ámbito.

1.2.2 CATEGORÍAS DE LOS DATOS PERSONALES

En el ámbito de la protección de datos, es fundamental entender los diversos tipos de datos personales que pueden ser objeto de tratamiento. Siendo la clasificación de estos datos algo fundamental no solo para determinar el nivel de protección necesario, sino que también para la forma en que deben ser gestionados y tratados conforme a la legislación vigente. Estas categorías establecen características específicas y requisitos de tratamiento que responden a su naturaleza y sensibilidad. De esta manera, para el análisis dentro del Ecuador, se debe remitir a las cuatro categorías que establece la Ley Orgánica de Protección de datos personales.

A.) DATOS SENSIBLES: El concepto de datos sensibles está definido en la Ley Orgánica de Protección de Datos. En esta se llega a definir en el artículo 4[4] en el cual se los enmarca en una categoría más específica de datos, los cuales están relacionados con los aspectos más íntimos de las personas. Siguiendo esta línea de ideas, el concepto que da esta norma puede ser respaldada por la OEA, donde la misma desarrolla que estos datos pertenecen a la esfera más íntima en el cual las personas se pueden llegar a desarrollar, en este sentido establece que dependiendo del contexto cultural, social o político, esta categoría puede incluir, entre otros, datos sobre la salud personal, preferencias sexuales o vida íntima, creencias religiosas, filosóficas o morales, afiliación sindical, información genética, datos biométricos ,que sirven para la identificación única de una persona, opiniones políticas, origen racial o étnico, información de cuentas bancarias, documentos oficiales, datos de menores de edad o geolocalización personal (Organización de los Estados Americanos, 2022).

Esto se puede abordar desde un punto de vista legal, donde se debe hacer énfasis en que, en muchas jurisdicciones, los datos personales sensibles requieren un tratamiento más estricto y tienen mayores restricciones respecto a su recopilación, almacenamiento, y procesamiento, debido a su potencial para causar discriminación u otros perjuicios, en el caso de ser divulgados o mal manejados. Entendiéndose, que este tipo de datos están más relacionados con la intimidad de las personas.

[4] Art. 4 .- Términos y definiciones.- Para los efectos de la aplicación de la presente Ley se establecen las siguientes definiciones: Datos sensibles: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales. ” (Ley Orgánica De Protección De Datos Personales, 2021).

En este contexto, es importante señalar que la Ley Orgánica de Protección de Datos impone restricciones más rigurosas al tratamiento de los datos personales sensibles, prohibiendo su manejo en la mayoría de los casos. Sin embargo, la misma ley contempla siete excepciones específicas bajo las cuales es posible tratar estos datos. Como primero, siempre está el consentimiento del titular de los datos, dicho consentimiento debe ser expreso y tiene que estar claramente establecido para que vaya a hacer tratados estos datos personales, prohibiendo así cualquier otro fin que sea para el cual se pactó.

De esta forma, el encargado de los datos personales es quien debe obtener el consentimiento del titular de los datos que van a hacer tratados, este consentimiento es recogido por el responsable del manejo de datos. Quien tiene la obligación de previamente y de manera precisa, informar al titular tanto el tiempo como la forma que estos datos van a hacer utilizados, pues así lo dispone el artículo 5[5] del Reglamento de la Ley Orgánica de Datos Personales.

El consentimiento debe manifestarse claramente a través de una declaración expresa por parte del titular de los datos, para que el responsable del tratamiento pueda demostrar que dicho consentimiento fue otorgado. Es fundamental señalar que ni el silencio ni la inacción del titular pueden interpretarse como una aceptación implícita.

Se debe establecer que el titular de los datos personales tiene el derecho de revocar el consentimiento otorgado en cualquier momento que este así lo decida. Además, de la forma que se protege al titular de los datos, también se protege al encargado del tratamiento de estos. Ya que una vez revocado el consentimiento, esto de ninguna forma afecta a la licitud del tratamiento de los datos llevados a cabo hasta el momento de la revocatoria.

Como segundo caso, para que se permita el tratamiento de estos datos. Cuando sea necesario el tratamiento en los ámbitos laborales y de seguridad social, se debe justificar que es esencial para cumplir con obligaciones legales o ejercer derechos específicos, ya sea por parte del empleador (responsable del tratamiento) o del empleado (titular de los datos).

Así por un lado, se tiene el ámbito laboral, donde los empleadores a menudo necesitan recopilar y procesar datos sensibles de sus empleados para cumplir con diversas

[5] Art. 5.- De la recogida del consentimiento. - el responsable deberá informar previa y detalladamente los tipos de tratamiento, finalidades, el tiempo de conservación, las medidas de protección a adoptarse, las consecuencias de su entrega, entre otros aspectos determinados en la Ley, lo cual deberá ser consentido inequívocamente por el titular. (REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2023).

obligaciones legales. Por ejemplo, está el cumplimiento de normativas como las de salud y seguridad en el trabajo, que vendría a hacer el caso de los exámenes médicos ocupacionales que aseguran que los empleados son aptos para realizar sus funciones.

Y por otro lado, en el contexto de la seguridad social, el tratamiento de datos personales sensibles es necesario para gestionar prestaciones y beneficios que los trabajadores tienen derecho. Como por ejemplo, el caso de las pensiones y jubilaciones. En este sentido se da un tratamiento de datos relacionados con la edad, el historial laboral y las condiciones médicas que puedan influir en la elegibilidad para la jubilación o pensión por invalidez.

Como tercer supuesto, se hace referencia a la Ley Orgánica de Datos Personales, en el artículo 26 literal C[6], donde el tratamiento de datos personales sensibles es necesario en situaciones en las que está en juego la protección de intereses vitales; siendo una excepción en la normativa de protección de datos. De esta forma, se permite a los responsables del tratamiento actuar en situaciones de emergencia para proteger la vida o la integridad de una persona, cuando ésta no puede dar su consentimiento. Este tipo de tratamiento está justificado por la necesidad imperiosa de proteger derechos fundamentales y se rige por los principios de proporcionalidad y necesidad.

Como cuarto supuesto, están los datos personales que su titular los ha hecho públicos, sin restricciones de acceso. Esto puede ocurrir a través de diferentes medios, como publicaciones en redes sociales, blogs personales, declaraciones en medios de comunicación, o cualquier otra plataforma pública. El quinto supuesto expone, el tratamiento de datos mediante una orden judicial. Esta excepción permite así que los datos personales, incluidos los datos sensibles, sean tratados sin el consentimiento del titular cuando existe una orden judicial que así lo disponga.

El sexto apartado establece que el tratamiento de datos sensibles es necesario cuando se dan tres supuestos:

a. Interés Público: El tratamiento de datos sensibles para fines de archivo dentro del interés público, se refiere a la conservación de información relevante para el beneficio general de la sociedad. Esto puede incluir archivos históricos, registros públicos, o información relevante para la administración pública.

[6]Arts. 4 .- Tratamiento de datos sensibles.- Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias: C) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento. (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021).

b. Investigación científica: pueden ser tratados para avanzar en el conocimiento en áreas científicas o históricas. Por ejemplo, estudios médicos que requieren acceso a datos históricos de pacientes o investigaciones históricas sobre eventos pasados.

c. Fines Estadísticos: El tratamiento para fines estadísticos implica el uso de datos para generar estadísticas que pueden informar sobre políticas públicas, estudios de mercado, o investigaciones académicas. Sin embargo, cabe señalar que estos datos en la mayoría de los casos si llegan a ser recolectados, deben ser anonimizados para proteger la identidad del individuo.

Y como ultimo supuesto está, el tratamiento de los datos de salud, porque si bien la Ley Orgánica les otorga una categoría especial, estos datos se los consideran como sensibles debido a que pertenecen a la esfera más personal de los individuos.

B.) DATOS DE NIÑAS, NIÑOS Y ADOLESCENTES: a breves rasgos, Los datos personales de niñas, niños y adolescentes requieren un tratamiento especial y riguroso debido a su vulnerabilidad y a la necesidad de proteger sus derechos fundamentales. Esto debido a su condición dada por el Código De La Niñez Y Adolescencia de *sujetos protegidos.* En donde, se los reconoce a tener una vida privada sin intromisiones de ningún tipo.

C.) DATOS DE SALUD: Dado que por su naturaleza estos datos incluyen información sobre el estado de salud, diagnósticos, tratamientos, historiales médicos y cualquier otra información relacionada con la salud de una persona. El manejo de estos datos requiere una atención especial para garantizar su confidencialidad, seguridad y uso ético.

En este sentido, la confidencialidad como principio trascendental que establece el Ministerio de Salud Pública, la cual se define como la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implica el conjunto de acciones que garantizan la seguridad en el manejo de esa información (Ministerio De Salud Pública, 2021).

De esta forma, cuando se dé el manejo de datos personales siempre se lo hace bajo la confidencialidad y el secreto profesional. La Ley Orgánica de Protección de datos establece, así, que como parámetro para dar tratamiento a estos datos personales, los mismos deben ser anonimizarlos o seudonimizarlos, siendo crucial en el tratamiento de datos de salud debido a la sensibilidad inherente a esta información.

D.) DATOS DE PERSONAS CON DISCAPACIDAD Y DE SUS SUSTITUTOS, RELATIVOS A LA DISCAPACIDAD: abreves rasgos, este tipo de datos deben recibir un tratamiento, especial debido a que están relacionados con la salud de las personas. Es fundamental aplicar principios de protección de datos para asegurar que esta información se utilice de manera ética y adecuada, respetando los derechos y la dignidad de las personas involucradas. Las leyes y normativas de protección de datos establecen directrices específicas para el tratamiento de estos datos, con el objetivo de proteger la privacidad y garantizar que las personas con discapacidad reciban el apoyo y la protección que merecen.

1.2.3 AUTORIDAD, RESPONSABLES Y ENCARGADOS DE TRATAMIENTO DE DATOS

En el ámbito de la protección de datos personales, es fundamental entender el rol tanto de la autoridad, los responsables y encargados del tratamiento de datos. Siendo estos quienes tienen un rol crucial en la gestión, protección y uso de la información personal.

Para ello es necesario remitirse a la Ley Orgánica de Protección de datos personales, la cual en el artículo 4 [7]dispone que la autoridad debe operar de manera autónoma, sin interferencias externas, especialmente del gobierno u otras entidades, para garantizar la imparcialidad en la supervisión y aplicación de la Ley Orgánica de Protección de Datos. Así, se debe empezar por la definición de la autoridad de datos personales:

Su importancia recae en que siendo el órgano principal para el control y vigilancia de los datos personales, es quien garantiza la protección de estos. Tomando acciones directas para que se respeten y se cumplan los derechos y garantías previstos tanto en la ley de protección de datos como en la misma constitución. Entre sus principales atribuciones están:

A. Supervisar, controlar y evaluar las actividades que realicen tanto los responsables como los encargados del tratamiento de datos personales.

B. Ejercer la potestad sancionadora tanto para los responsables, encargados y los terceros quienes tengan bajo su poder el tratamiento de datos.

C. Es quien resuelve los reclamos que sean interpuestos por el titular de datos.

[7] Art. 4 .- Términos y definiciones.- Para los efectos de la aplicación de la presente Ley se establecen las siguientes definiciones: Autoridad de Protección de Datos Personales: Autoridad independiente encargada de supervisar la aplicación de la presente Ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales. . (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021).

D. Se le otorga la potestad para emitir normativa técnica ,así como criterios.

De esta forma, es quien dirige el registro nacional de protección de datos personales, coordinando así las acciones que sean necesarias para la protección de estos, tanto en el ámbito privado como el público.

Por otro lado, están los responsables del tratamiento de los datos personales, quienes pueden ser personas naturales o cualquier entidad tanto del sector público como privado; sobre ellos recae la responsabilidad de decidir tanto la finalidad (el "porque" se trata la información) como la manera en que se llevará a cabo ese tratamiento (el "cómo"). Estas decisiones son fundamentales para determinar si el tratamiento es adecuado y legal bajo las normativas de protección de datos.

Cabe mencionar que dentro del manejo de datos personales también están los delegados de la protección de datos, quienes son únicamente personas naturales que se encargan de otorgar la información sobre el tratamiento de datos al responsable. Además, son quienes supervisan el cumplimiento normativo en materia de protección de datos.

Estas personas tienen la responsabilidad de asesorar tanto al responsable del tratamiento (quien determina cómo y porque se tratan los datos) como al encargado del tratamiento (quien gestiona los datos bajo la dirección del responsable), sobre sus deberes legales en materia de protección de datos. Sin embargo, más allá de informar, esta persona tiene la tarea de supervisar que la organización cumpla efectivamente con las leyes de protección de datos. Esto incluye la implementación de políticas, la revisión de procesos y la realización de auditorías internas para garantizar el cumplimiento.

El individuo también actúa como intermediario entre la organización y la autoridad reguladora de protección de datos. Este rol implica colaborar en inspecciones, proporcionar información y ayudar a resolver cuestiones relacionadas con el cumplimiento de las normativas. Finalmente, el delegado de Protección de Datos es el enlace directo entre la entidad que maneja los datos y la autoridad reguladora. Este punto de contacto es crucial para la comunicación fluida y la resolución de problemas relacionados con la protección de datos.

Y por último, se encuentran los encargados de la protección de datos, a quienes se les designa para gestionar los datos a nombre del responsable del tratamiento. Este rol puede ser asumido por personas naturales hasta organizaciones grandes, además da la posibilidad de la cooperación con otras entidades; cabe resaltar que el encargado no determina los fines del tratamiento, sino que actúa según las instrucciones del

responsable, asegurando que los datos se manejen de acuerdo con las normativas aplicables.

CAPÍTULO 2

2.1. MANEJO DE DATOS PERSONALES POR PARTE DE LAS ENTIDADES FINANCIERAS: PROCEDIMIENTOS PARA EL COBRO DE OBLIGACIONES

Las entidades financieras, en su rol de intermediarios en el sistema económico, manejan diariamente una gran cantidad de información personal y financiera de sus clientes. Estos datos, que incluyen desde información de contacto hasta detalles sobre transacciones y patrones de consumo, son fundamentales para el desarrollo de sus operaciones y la prestación de servicios personalizados.

El manejo de estos datos conlleva una gran responsabilidad, dado que la naturaleza sensible de la información financiera puede tener consecuencias significativas si se utiliza de manera indebida o si no se protege adecuadamente. Por esta razón, es importante que las entidades financieras se encuentren sujetas a un riguroso marco normativo que regule cómo deben recopilar, procesar, almacenar y compartir los datos personales de sus usuarios, teniendo así como objetivo principal proteger la privacidad de los individuos, garantizando que sus datos se manejen de manera ética y segura.

2.1.1 IMPORTANCIA DE LA RELACIÓN USUARIO-ENTIDAD FINANCIERA

La relación entre el usuario y la entidad financiera es un pilar fundamental en el funcionamiento del sistema financiero. Esta interacción no solo se basa en la prestación de servicios, sino que también implica un vínculo de confianza, transparencia, y responsabilidad mutua. La importancia de esta relación radica en su impacto directo en la estabilidad financiera individual y colectiva, así como en la eficiencia y la solidez del sistema en su conjunto.

Así, en la codificación de la Superintendencia De Bancos Libro Primero Tomo IV. Donde se dispone la obligación de las entidades financieras de salvaguardar y defender tanto los derechos como los intereses de los usuarios , que hacen uso de los productos ofrecidos por las entidades financieras, ya sean del sector público o privado. Busca Garantizar en debida forma que no se den prácticas fraudulentas o prohibidas.

En este contexto, el artículo 14[8] de la mencionada codificación establece que una de las obligaciones fundamentales de las entidades supervisadas es la protección de los datos de los consumidores, con el fin de preservar la confidencialidad de la información proporcionada por estos. En este sentido, existe una figura clave dentro del sistema financiero para la protección de la privacidad de los usuarios, conocida como el sigilo bancario.

Este principio constituye el pilar fundamental sobre el cual se asienta la confianza del usuario en la entidad financiera, garantizando que sus derechos e intereses sean debidamente protegidos en el marco de la relación contractual. Tomando como referencia a la autora Azaustre, la misma establece que la obligación de confidencialidad y discreción debe ser aplicada por las entidades financieras respecto a las operaciones que le han sido confiadas por el cliente (Azaustre, 2008). Por otro lado, para los autores Bartels y Arias, el sigilo bancario tiene como fundamento el secreto profesional. Donde se argumenta que, así como algunas profesiones exigen confidencialidad de quienes prestan el servicio, el secreto bancario es esencial para la actividad de las entidades financieras (Villanueva y Arias, 2010). Además, se debe subrayar que este secreto es una obligación jurídica para los bancos, derivada de la relación contractual.

Al analizar los conceptos expuestos tanto por la autora Azaustre, como por los autores Bartels y Arias, se evidencian dos enfoques complementarios sobre el sigilo bancario, ambos fundamentales en el ámbito financiero. Ambos enfoques coinciden en que el sigilo bancario es esencial para la confianza del usuario en la entidad financiera. En conjunto, estos conceptos subrayan la importancia de la confidencialidad como un pilar fundamental en la relación entre el banco y el cliente, reflejando tanto la ética profesional como la responsabilidad jurídica que dicha relación implica.

Por otro lado, se tiene al sigilo bancario desde el punto de vista como *deber*. De esta forma, para los autores Villanueva y Arias las entidades crediticias tienen la obligación de no revelar información sobre las cuentas de sus clientes ni sobre otros hechos conocidos a través de sus actividades, a menos que la ley disponga lo contrario (Villanueva y Arias, 2010).

[8] Art. 14 .- Protección de la privacidad.- Las entidades controladas deben proteger los datos de los consumidores y/o beneficiarios a fin de mantener la confidencialidad de la información personal recibida. (Superintendencia De Bancos, 2024).

De esta manera, se puede concluir que la confidencialidad es un deber que recae sobre las instituciones financieras, haciendo referencia a la obligación de no revelar información sobre las actividades que sus usuarios realicen con ellas. Sin embargo, cabe recalcar que el punto de vista de los autores antes citados, si bien hacen referencia a una obligación, en el fondo los tres autores llegan a la misma conclusión, siendo este principio algo fundamental para incrementar y fortalecer la confianza que depositan los usuarios hacia las entidades financieras.

El sigilo bancario no se limita a un enfoque meramente doctrinario, sino que está consagrado en la Constitución de la República del Ecuador, específicamente en el artículo 66, numeral 21, que garantiza la confidencialidad de la información perteneciente a la esfera privada de los individuos. Este precepto impide tanto al estado como a particulares acceder directamente a dicha información, lo cual guarda una estrecha relación con lo establecido en la Ley Orgánica de Protección de Datos Personales. En este contexto, las entidades financieras, como responsables del tratamiento de datos, deben no solo definir los métodos de procesamiento, sino también implementar medidas que aseguren el cumplimiento efectivo de los principios de protección deditos los derechos reconocidos en la normativa vigente.

Así mismo, el Código Orgánico Monetario y Financiero dentro del libro I, en su artículo 255 numeral 13[9] dispone que las entidades financieras tienen prohibido vulnerar el sigilo bancario. En este contexto, dentro del marco legal ecuatoriano, tanto a nivel constitucional como en leyes orgánicas, se establece con claridad las obligaciones y las prohibiciones que tienen las entidades financieras , con el objetivo de proteger la confidencialidad de la información de sus clientes. Este deber de sigilo no solo es un pilar de la relación de confianza entre el cliente y la entidad financiera, sino también un imperativo legal que, de ser incumplido, puede acarrear severas consecuencias para las instituciones. La normativa vigente exige que las entidades implementen mecanismos eficaces para garantizar la protección de los datos personales, alineándose con los principios de protección de datos y asegurando el respeto a los derechos fundamentales consagrados en la Constitución.

¿Cómo se garantiza, entonces, la aplicación del sigilo bancario? En este contexto, la Codificación de la Superintendencia de Bancos establece lo que se conoce como

[9] Art. 255 .- Prohibiciones a entidades del sistema financiero nacional. Se prohíbe a las entidades del sistema financiero nacional: 13. Violar el sigilo o la reserva. (CÓDIGO ORGÁNICO MONETARIO Y FINANCIERO, LIBRO I, 2024).

políticas de privacidad, las cuales son implementadas mediante procedimientos internos por parte de las entidades financieras para salvaguardar la privacidad de los datos personales de los usuarios. Estas políticas constituyen un elemento esencial en el cumplimiento de las normativas sobre protección de datos personales. Formalizadas por escrito, no solo reflejan el compromiso de la entidad con la confidencialidad, sino que también constituyen un requisito legal y regulatorio.

Desde una perspectiva de derecho bancario, estas políticas y procedimientos deben estar alineados con las mejores prácticas del sector, así como con las exigencias impuestas por la legislación vigente, con el objetivo de establecer un marco operativo claro y efectivo que permita a las entidades financieras gestionar, almacenar y procesar la información sensible de los usuarios de manera segura y siempre conforme a los principios ya analizados de integridad, confidencialidad y disponibilidad de los datos.

2.1.2 MANEJO DE DATOS PERSONALES: ENTIDADES FINANCIERAS

Las entidades financieras gestionan una cantidad considerable de datos personales de sus usuarios, que incluyen información financiera, historial crediticio y datos de identificación. El manejo inadecuado de esta información no solo compromete la seguridad y la privacidad de los usuarios, como se analizó anteriormente, sino que también expone a las instituciones a serias repercusiones. Además, las entidades que no cumplen con las normativas de protección de datos pueden enfrentarse a sanciones legales.

Así, como se estableció con anterioridad para el manejo de protección de datos existe la autoridad, los responsables y los delegados. En este caso, las entidades financieras toman el rol de responsables del manejo de datos personales, es decir, tienen la autoridad, ya sea de manera individual o en colaboración con otros, para decidir sobre los fines y la forma en que se manejan estos datos.

Para los fines de este análisis, es necesario examinar la responsabilidad de las entidades financieras en el manejo de datos personales, así como los objetivos específicos para los cuales se procesan dichos datos. Sin embargo, debido a consideraciones legales, se hará referencia a estas entidades de manera anónima, denominándolas Institución Financiera “A”.

De este modo, para analizar el tratamiento de datos por parte de la Institución Financiera es necesario dividirlo en cuatro partes. La primera, es la política de protección y privacidad , en cuanto a su aplicación, siendo un paso fundamental para cumplir con las normativas de protección de datos vigentes y demostrar su compromiso con la privacidad

de sus usuarios. Al designarse a sí misma como responsable del tratamiento de datos, la Institución "A" asume la obligación legal de garantizar que los datos personales sean gestionados de acuerdo con los principios de legalidad, finalidad, transparencia y proporcionalidad.

Como segundo está el alcance que tiene dicha política de protección de datos. Es importante este punto debido a que, la Institución Financiera "A" no se limita a las acciones de la propia institución, sino que se extiende a todos los colaboradores y personas vinculadas a ella. Este enfoque es esencial, ya que reconoce que la seguridad de los datos personales no solo depende de la entidad principal, sino también de terceros que, de alguna manera, manejan o accedan a estos datos. Por lo tanto, la institución impone una responsabilidad compartida, asegurando que todos los actores involucrados estén obligados a respetar las mismas normas de protección y privacidad.

El tercer punto de este análisis se conecta con el realizado anteriormente, ya que se mencionó a la responsabilidad que no solo ostenta la Institución “A”, sino terceros relacionados. Bien sean estos personas naturales o jurídicas, que tengan en su poder bases de datos asociadas a la Institución Financiera "A", tienen la obligación de tratar esos datos de manera transparente , respetando de esta forma la privacidad de los usuarios. Esta disposición implica que cualquier manejo indebido, fuga o uso no autorizado de los datos puede dar lugar a responsabilidades legales tanto para la institución como para los individuos o entidades que los gestionen. En este sentido, la institución no solo cumple con la normativa de protección de datos a nivel interno, sino que también extiende su obligación de protección a través de acuerdos contractuales con terceros.

El cuarto punto es la transparencia con la que la institución “A” debe manejar los datos personales que estén bajo su poder, implicando que los titulares de los datos personales deben ser informados de manera clara sobre cómo y para qué se están utilizando sus datos. La Institución Financiera "A" tiene la responsabilidad de comunicar a sus usuarios las finalidades del tratamiento de datos, los derechos que tienen respecto a sus datos y las medidas de seguridad que se han implementado para protegerlos.

Esta política de protección de datos es fundamental, ya que impone a las entidades financieras la obligación esencial de informar a los titulares acerca de quién es responsable del tratamiento de sus datos personales. Es crucial establecer de manera clara quién tiene la autoridad para decidir y controlar el uso de dicha información, asegurando así la transparencia y el cumplimiento de las normativas de protección de datos. De esta

manera, el titular de la información puede otorgar su consentimiento de manera informada, con pleno conocimiento de quién gestionará sus datos.

2.1.3 FACULTADES OTORGADAS A LAS ENTIDADES FINANCIERAS POR LA NORMA PARA EL COBRÓ DE OBLIGACIONES

Ahora bien, en el contexto sobre el cobro de obligaciones por parte de las entidades financieras , se debe entender que los datos crediticios forman parte de lo que se conoce como datos personales, pues así lo establece La Ley Orgánica de Protección de Datos personales en el artículo 4[10], en donde los datos personales crediticios se refieren a la información que refleja el comportamiento económico de individuos; mismos que en el contexto financiero son utilizados para evaluar su capacidad para el cumplimiento de obligaciones. Este tipo de datos incluye, información sobre el historial de crédito, el cumplimiento de obligaciones de pago, los ingresos y los activos financieros de la persona. Su principal propósito es suministrar una visión integral de la situación económica del individuo, lo cual es esencial para la toma de decisiones en el ámbito financiero, como la aprobación de préstamos, la concesión de líneas de crédito, y otras operaciones financieras.

De esta forma, estos datos tienen 3 componentes. Primero está el historial crediticio que hace referencia al registro de cuentas de crédito abiertas en los cuales constan tanto los pagos realizados como los pagos atrasados. Es decir, este historial refleja como el usuario financiero ha manejado sus obligaciones dentro de un periodo de tiempo. Como segundo, se debe tomar la capacidad de pago, en otras palabras, esto refleja el compromiso de las personas para dar cumplimiento a sus obligaciones financieras. Como tercero, se debe incluir las obligaciones actuales, bien sean préstamos, tarjetas de crédito otros compromisos que el usuario se obligó a cumplir a la institución financiera.

Estos datos son fundamentales para evaluar la solvencia y el riesgo asociado a los usuarios que quieran acceder a los servicios financieros. Las entidades financieras utilizan esta información para determinar la probabilidad de que un individuo pueda cumplir con sus obligaciones crediticias en el futuro. De esta forma, un análisis detallado de estos datos ayuda a las instituciones a tomar decisiones informadas sobre la concesión de

[10] Art. 4.- Términos y definiciones.- Para los efectos de la aplicación de la presente Ley se establecen las siguientes definiciones:
Datos personales crediticios: Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera. (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES,2021).

crédito y a establecer condiciones adecuadas para el otorgamiento de productos financieros.

Ahora bien, entendiendo esto la Ley Orgánica de Protección de Datos Personales en el artículo 28[11] establece por un lado el tratamiento legítimo de los datos personales crediticios cuando estos sean destinados a informar sobre la solvencia patrimonial o crediticia, considerado legítimo y lícito esta práctica. Esta legitimidad tiene como base la necesidad de evaluar la capacidad de pago del titular de los datos, la conducta comercial, y la posibilidad de concretar negocios. Esta justificación permite que las entidades financieras y comerciales analicen la situación económica de una persona para tomar decisiones informadas sobre la concesión de crédito o la celebración de contratos.

Sin embargo, el tratamiento de estos datos tiene una finalidad específica, siendo que los datos crediticios deben ser utilizados exclusivamente con la finalidad para el análisis de solvencia patrimonial o crediticia. Esto significa que la información recopilada no puede ser utilizada para otros propósitos distintos a los establecidos, como la evaluación de la capacidad de pago o la conducta comercial del titular, evitando de esta forma que los mismos sean utilizados para actividades no autorizadas o en beneficio de terceros.

Esto tiene como límite la comunicación o difusión de los datos crediticios, así como cualquier uso para fines secundarios. Esta disposición protege la privacidad del titular de los datos al evitar que su información sea compartida sin su consentimiento o utilizada para otros propósitos no relacionados con el análisis crediticio.

Por otro lado, el artículo 18[12] del reglamento de la Ley Orgánica De Protección de Datos personales, complementa la idea de su ley, desde un punto de vista de los datos crediticios como medio de información sobre el cumplimiento o incumplimiento de

[11] Art. 28.- Datos crediticios.- Salvo prueba en contrario será legítimo y lícito el tratamiento de datos destinados a informar sobre la solvencia patrimonial o crediticia, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor. Tales datos pueden ser utilizados solamente para esa finalidad de análisis y no serán comunicados o difundidos, ni podrán tener cualquier finalidad secundaria. Datos personales crediticios: Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera. (LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2021).

[12] Art. 18.- De los datos crediticios. - A efectos de lo dispuesto en la Ley, será lícito el tratamiento de datos personales que tenga como fin informar sobre el cumplimiento o incumplimiento de obligaciones comerciales o crediticias. La Junta de Política y Regulación Financiera, como organismo de regulación, y la Superintendencia de Bancos, como organismo de control, regularán la protección de los datos crediticios, en el ámbito de sus competencias. (REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, 2023).

obligaciones comerciales o crediticias. Esto implica que las entidades financieras y comerciales tienen una base legal para manejar estos datos con el objetivo específico de evaluar como una persona ha cumplido con sus obligaciones financieras. Estableciendo así una visión clara sobre la situación crediticia de las personas; siendo esto vital para la toma de decisiones relacionadas con la concesión de crédito, la celebración de contratos, y la evaluación del riesgo financiero.

2.1.4 COMPAÑÍAS DE SERVICIOS AUXILIARES DE COBRANZA DE CARTERA: FUNCIONES Y ROL EN LA GESTIÓN DE CRÉDITOS

En el ámbito financiero y comercial, la gestión efectiva de créditos y la recuperación de obligaciones son fundamentales para mantener la economía de las instituciones y empresas. Las compañías de servicios auxiliares de cobranza y generación de cartera juegan un papel esencial en este proceso, ofreciendo especialización y apoyo crucial en la administración de cuentas por cobrar. Estás entidades se encargan no solo de la recuperación de deudas pendientes, sino también de la generación y análisis de datos crediticios que permiten una evaluación precisa del riesgo y la capacidad de pago de los usuarios. Las compañías de servicios auxiliares de cobranza se enfocan en la gestión y recuperación de deudas vencidas, implementando estrategias efectivas para negociar con los deudores y asegurar el cobro de los montos adeudados. De esta forma, Gestionan el cobro de las cuentas vencidas a través de diversos métodos, que pueden incluir llamadas telefónicas, cartas de demanda, y negociaciones con los deudores.

Las compañías de servicios auxiliares de cobranza y/o generación desempeñan un papel crucial en el sistema financiero al facilitar la recuperación dedeadas proporcionar información esencial para la toma de decisiones crediticias. Su trabajo ayuda a las entidades financieras a gestionar eficazmente el riesgo crediticio y a mejorar la eficiencia en la recuperación de pagos pendientes.

En el contexto financiero estas compañías son de suma importancia, debido a que las instituciones financieras disponen de la facultad de transferencia, comunicación y acceso a los datos personales. Esto se dispone en el artículo 33[13] de la Ley Orgánica de

[13] Art. 33.- Transferencia o comunicación de datos personales. - Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente real clonados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada dentro de una de las causales de legitimidad establecidas en esta Ley, y se cuente, además, con el consentimiento del titular. Se entenderá que el consentimiento es informado cuando para la transferencia o comunicación de datos personales el responsable del tratamiento haya entregado información suficiente al titular que le permita conocer la finalidad a que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos. (la Ley Orgánica de Protección de Datos Personales, 2021).

Protección de Datos Personales, siendo esto algo validó siempre y cuando esté directamente relacionado con fines vinculados con las funciones legítimas tanto del responsable del tratamiento como del destinatario. Esto garantiza que la información no se transfiera sin un propósito claro y legítimo que esté alineado con las responsabilidades de ambas partes.

En este contexto, las instituciones financieras que proporcionan servicios financieros, como la concesión de créditos, tienen la facultad de exigir a sus usuarios la devolución de estos. Paralelamente, las compañías auxiliares de cobranza permiten a las instituciones financieras obtener liquidez mediante la venta de carteras. Estás compañías auxiliares, al asumir la facultad de cobro de las obligaciones, reciben los datos personales de los deudores para gestionar el proceso de recuperación de deudas.

Este esquema implica que tanto las instituciones financieras como las compañías auxiliares manejan datos personales de los deudores, lo cual debe hacerse conforme a las normativas de protección de datos vigentes, garantizando la transparencia y el respeto a la privacidad de los titulares de la información.

En este sentido, los datos personales de los deudores han sido trasladados a estas compañías, teniendo así la responsabilidad de establecer políticas y procedimientos documentados apropiados para gestionar y prevenir de manera efectiva los riesgos que puedan comprometer los derechos de los consumidores financieros. Así pues, ahora las compañías auxiliares tienen la obligación de resguardar las bases de datos que les ha sido otorgadas por parte de los encargados de datos personales. Ahora tienen la obligación de cumplir únicamente con la finalidad para la cual el banco les otorgó esos datos, de esta forma, es exclusivamente para el cobro de las obligaciones pendientes de pago por parte de los usuarios financieros. Siendo que, para la recopilación de los datos personales que sean otorgados a las compañías auxiliares, permite que las entidades financieras controladas suscriban con las compañías de servicios auxiliares políticas de privacidad. Estas políticas tienen como objetivo garantizar la protección adecuada de los datos personales de los usuarios financieros; asegurando que las prácticas de manejo de datos sean conformes a las regulaciones y estándares establecidos.

Esto implica que las políticas suscritas deben abordar la protección de datos. Esto incluye la implementación de medidas técnicas y organizativas para prevenir accesos no autorizados, fugas de información y otros riesgos que puedan comprometer la

confidencialidad y la integridad de los datos. Pues así lo establece La Codificación de la Superintendencia De Bancos, Libro Primero Tomo I en el artículo 25 [14].

La recopilación y el uso de datos personales deben respetar los derechos de privacidad, intimidad y confidencialidad, siempre que dichos usos cuenten con la debida autorización del titular. Ahora bien, ¿cómo otorga el titular su consentimiento? Como se mencionó anteriormente, este debe ser otorgado por escrito. En el caso de las instituciones financieras, el consentimiento se formaliza a través del contrato de adhesión emitido por la entidad y aceptado por el titular.

2.2. CONTRATO DE ADHESIÓN

En el ámbito de los contratos comerciales y financieros, el contrato de adhesión emerge como un instrumento fundamental que regula las relaciones entre las partes involucradas. A diferencia de los contratos negociados bilateralmente, el contrato de adhesión se caracteriza por ser elaborado por una de las partes de manera unilateral, estableciendo términos y condiciones a los cuales la otra parte debe adherirse sin posibilidad de negociación. Este tipo de contrato es común en diversos sectores, incluyendo el financiero, el de seguros y el de servicios públicos, donde las condiciones estandarizadas facilitan la prestación eficiente y uniforme de servicios.

El tratadista Guillermo Cabanellas establece que los contratos de adhesión se basan en la participación de un acto efectuado por un tercero, donde se da la aceptación de condiciones contractuales establecidas unilateralmente por una de las partes, sin posibilidad de negociación (Cabanellas, 2006).En este contexto, la colaboración implica que una de las partes participa en un acuerdo o acto que ha sido establecido por otra parte. Esta colaboración suele ser necesaria para llevar a cabo el contrato, ya sea que se trate de la prestación de servicios, la adquisición de bienes, o el cumplimiento de una obligación.

La aceptación de reglas contractuales impuestas por una de las partes significa que el adherente acepta los términos y condiciones establecidos por la otra parte sin tener la posibilidad de negociar o modificar esos términos. En un contrato de adhesión, el proponente redacta el contrato y presenta los términos de manera unilateral, dejando al adherente la opción de aceptarlos en su totalidad o rechazar el contrato en su conjunto.

[14] Art. 25.- Las entidades financieras controladas, de ser el caso, podrán suscribir con las Compañías de Servicios Auxiliares, una Política de Privacidad y Seguridad de Infraestructura Tecnológica, entre otros que contribuyan a la protección de los datos de los consumidores financieros. El incumplimiento de estas disposiciones será sancionado con la suspensión temporal, en caso de que este sea reiterativo será sancionado con la descalificación de conformidad a lo dispuesto en la Sección III de esta norma. (CODIFICACIÓN SUPERINTENDENCIA DE BANCOS, LIBRO PRIMERO TOMO I, 2024).

Siendo un contrato que se establece sin discusión previa, cuando una de las partes acepta de manera directa las condiciones propuestas por la otra. Así, su rasgo distintivo es la falta de negociaciones preliminares entre las partes involucradas y en términos más comunes, una de las partes impone "las condiciones del contrato" al otro, quien solo tiene la opción de aceptar o rechazar dichas condiciones (Pardo, 2013).

En este sentido, los contratos financieros se configuran como un claro ejemplo de contratos de adhesión, caracterizados por la ausencia de una negociación bilateral efectiva. En dichos contratos, la entidad financiera establece unilateralmente los términos y condiciones, a los cuales los usuarios deben adherirse sin posibilidad de modificar sus cláusulas. No obstante, la formalización de estos contratos requiere un riguroso cumplimiento del marco legal aplicable, garantizando el respeto y la protección de los derechos de los clientes. Así, aunque prevalezca la voluntad de la entidad financiera en la redacción de los términos contractuales, estos deben alinearse con las normativas vigentes y los principios de equidad y transparencia en la relación con los consumidores.

Por su parte, la Superintendencia de Bancos define al contrato de adhesión el documento que contiene cláusulas predeterminadas por la entidad financiera, tanto del sector público como privado, y debe estar escrito con un tamaño de fuente no inferior a diez (10) puntos, de manera legible. Este debe alinearse con los estándares internacionales en términos informáticos, empleando un lenguaje claro y accesible. Además, no podrá hacer referencia a textos o documentos que no sean de acceso público y que no se entreguen al consumidor antes de formalizar el contrato. (Superintendencia de Bancos, 2024). De esta forma, se puede desglosar al a definición de esta institución en cinco principales partes:

1. **Claridad y Transparencia en los Contratos de Adhesión:** La disposición busca garantizar que los contratos de adhesión sean accesibles y comprensibles para el consumidor. Al exigir un tamaño de fuente mínimo de diez puntos y redacción en términos claros y comprensibles, se está promoviendo la transparencia y evitando cláusulas confusas o difíciles de entender, que podrían colocar al consumidor en desventaja.

2. **Legibilidad y Accesibilidad**: El requerimiento de utilizar un tamaño de fuente específico asegura que la información sea legible, evitando que se oculten términos importantes en letras pequeñas, lo que es común en algunos contratos para que los consumidores no noten cláusulas desfavorables.

3. **Prohibición de Remisiones a Documentos No Públicos:** La prohibición de incluir referencias a textos o documentos que no sean de conocimiento público, a menos que se faciliten previamente al usuario, siendo es una medida para proteger al mismo de cláusulas sorpresivas o inesperadas. Esto implica que todas las condiciones relevantes deben ser claramente accesibles y entendibles antes de que el usuario se comprometa contractualmente.

4. **Normas Informáticas Internacionales**: El hecho de que se mencionen las normas informáticas internacionales indica un intento de estandarizar la presentación de la información contractual, lo que puede ser particularmente relevante en contratos electrónicos o digitales. Esto asegura uniformidad y facilita la supervisión y cumplimiento por parte de las autoridades regulatorias.

5. **Protección del Consumidor:** En términos generales, estas disposiciones son una manifestación del principio de protección al consumidor, buscando equilibrar la asimetría de poder entre las instituciones financieras y los clientes. La normativa quiere evitar abusos y asegurar que los consumidores tomen decisiones informadas basadas en una comprensión completa de los términos contractuales.

2.2.1 CARACTERÍSTICAS

Si bien no existe un pleno consenso en la doctrina sobre las características que definen este tipo específico de contrato entre los diferentes autores. No obstante, entre las características más reconocidas por la doctrina se encuentran las siguientes:

1. **Redacción unilateral:** es decir, una de las partes es quien redacta el contenido del contrato, sin discutir el contenido de este con la otra parte. Para Carlos muñoz, en el contrato de adhesión una de las partes, denominada estipulante, establece de manera unilateral todas las condiciones del contrato, de modo que, al celebrarse, la relación jurídica patrimonial generada refleja únicamente la intención del oferente (Muñoz, 2018). Es decir, la parte que ofrece el contrato (generalmente una empresa o institución), establece de manera unilateral todos los términos y condiciones del acuerdo. En este tipo de contratos, el adherente (la otra parte) no tiene la oportunidad de negociar o modificar las cláusulas, limitándose únicamente a aceptar o rechazar las condiciones impuestas.

2. **La oferta no es negociable:** de esta forma, la posición del adherente se enfrasca netamente en rechazar o aceptar de manera íntegra todo lo que ha sido fijado por la otra parte, teniendo así requisitos impuesto únicamente por el ofertante.

3. **Dirigido a un amplio número de personas:** Esta característica se manifiesta en los contratos de adhesión debido a que no están destinados a una sola persona específica. En lugar de ello, están dirigidos a un público amplio, compuesto por múltiples individuos a quienes va dirigida la oferta del proveedor de servicios o productos.

4. **El estado de necesidad:** Para Melania Pardo esto hace referencia a la circunstancia en la que el aceptante o consumidor se ve forzado a dar su consentimiento ante un contrato cuyas condiciones han sido establecidas de manera unilateral por el oferente (Pardo, 2013). Esto calza de manera perfecta dentro del contexto financiero, debido a que los individuos se acercan a estas instituciones con el fin de cubrir con una necesidad que en este caso vendría hacer económica.

5. **Aceptación:** en estos contratos, el adherente si realiza una manifestación de la voluntad, expresando así la aceptación por contratar ese servicio que se le es ofrecido, teniendo así una expresión del consentimiento debidamente informado.

En este sentido, el manejo de datos personales vendría a hacer una de las cláusulas que las instituciones financieras imponen al momento de realizar contratos para acceder a sus servicios financieros. Es importante recalcar que al momento de realizar este análisis se tomaron varios contratos con el fin de analizar las cláusulas de manejo de datos, en las cuales básicamente coincidían en dos principales circunstancias. La primera es la revisión de los datos personales del usuario financiero, en los cuales implica que las instituciones financieras puedan acceder a los datos personales y dentro esto se estipula el tiempo de conservación, las finalidades del tratamiento de estos y además, los derechos que los titulares tienen sobre ellos, como por ejemplo, acceso, eliminación, ratificación y actualización de estos.

La segunda, trata sobre la transferencia que se puede realizar con estos datos hacia terceros, de esta forma, se autoriza una vez firmado el contrato que la entidad financiera puede realizar el traslado de los datos personales a terceras personas que como se analizó con anterioridad vendrían a ser las compañías de servicios auxiliares. De esta forma, si bien no se discuten las cláusulas establecidas dentro de estos contratos los titulares deben tener la información clara y precisa sobre cómo se va a llevar a cabo el manejo de sus datos.

2.2.2 PROHIBICIONES DE LOS CONTRATOS DE ADHESIÓN

Como bien se analizó con anterioridad, este tipo de contratos para su realización solo consta la voluntad de una de las partes. Sin embargo, dentro de la legislación ecuatoriana se limita este poder que tiene una de las partes, impidiendo que la misma imponga condiciones abusivas dentro del contrato.

Estableciendo tanto cláusulas abusivas como prohibidas, establecidas dentro de la Codificación Superintendencia De Bancos, Libro Primero Tomo IV en el artículo 4[15] . Haciendo referencia a las primeras, para ser analizadas deben ser divididas en cuatro partes:

1. **Principio de buena fe objetiva**: exige que las partes en un contrato actúen con honestidad y equidad. Las cláusulas abusivas, al ser desproporcionadas o injustas, violan este principio al imponer condiciones desleales sobre una de las partes, normalmente el consumidor o beneficiario, quien está en una posición de desventaja.

   Para la autora Roberta Lídice, en los contratos y con especial atención a los de consumo, este principio es de suma importancia entendiéndose que no es suficiente con cumplir con la obligación principal de un contrato, ya que, existen también obligaciones secundarias, conocidas como accesorias, que tienen igual relevancia y deben ser observadas debidamente (Lídice, 2018).

   En el contexto de los contratos financieros, especialmente los de crédito, no basta con que la institución se limite a otorgar el crédito. Es fundamental que también respete la privacidad del usuario y mantenga la confidencialidad sobre su situación financiera, cumpliendo así con el principio de sigilo bancario.

   La autora Lídice considera fundamental, para el cumplimiento del principio de buena fe, que se informe claramente cómo será ejecutado el contrato y cuáles son sus condiciones, es decir, que el proveedor debe cumplir con lo pactado y notificar debidamente al consumidor (Lídice, 2018). En cuanto a los datos personales, esto es crucial, ya que la institución financiera tiene la

[15] Art. 4.- Glosario. - Para los efectos de la aplicación de esta norma, se definen los siguientes términos:
Cláusulas abusivas.- Aquellas que se incluyen en los contratos y son contrarias al principio de buena fe y el justo equilibrio entre consumidores financieros y entidades de los sectores financieros público y privado, y beneficiarios del sistema de seguridad social con las entidades que lo integran, que no han sido negociadas libremente y de común acuerdo entre las partes
Cláusulas prohibidas. - Aquellas estipulaciones contractuales que implican limitación, perjuicio o renuncia a los derechos de los consumidores financieros. (CODIFICACIÓN SUPERINTENDENCIA DE BANCOS, LIBRO PRIMERO TOMO IV, 2024).

obligación de informar de manera precisa quién, cómo y para qué serán tratados los datos financieros del titular.

2. **Desequilibrio en la Relación Contractual:** Estas cláusulas generan un desequilibrio entre los derechos y obligaciones de las partes, favoreciendo desproporcionadamente al proveedor del servicio o entidad, y perjudicando al consumidor o beneficiario.

3. **Falta de Negociación Libre:** Las cláusulas abusivas suelen ser impuestas sin la posibilidad de negociación por parte del adherente. En los contratos de adhesión, por ejemplo, el consumidor acepta términos predefinidos sin opción a modificar las cláusulas, lo que puede dar lugar a condiciones que favorezcan excesivamente al ofertante y que no han sido pactadas de mutuo acuerdo.

4. **Contexto en el Sector Financiero y de Seguridad Social:** En el contexto financiero y del sistema de seguridad social, las cláusulas abusivas pueden manifestarse en términos que imponen cargas desproporcionadas a los consumidores o beneficiarios, tales como comisiones excesivas, penalidades desmedidas o limitaciones injustas en los derechos del usuario. La regulación en estos sectores busca prevenir y sancionar tales cláusulas para proteger a las partes más vulnerables.

Por otro lado, se tiene las cláusulas prohibidas, que al igual que las anteriores, se las pueden dividir en tres partes para realizar su análisis:

1. **Limitación de Derechos:** Las cláusulas prohibidas pueden incluir disposiciones que restringen derechos básicos de los consumidores financieros, como el derecho a recibir información clara y precisa, el derecho a reclamar o a obtener un trato equitativo. Estas limitaciones pueden socavar la capacidad del consumidor para hacer valer sus derechos y buscar soluciones en caso de conflictos contractuales.

2. **Perjuicio a los Derechos:** Además de limitar derechos, estas cláusulas pueden causar un perjuicio directo al consumidor. Esto puede manifestarse en forma de penalidades desmedidas, comisiones ocultas, o condiciones que desproporcionadamente favorecen al proveedor del servicio, en detrimento del bienestar y los intereses del consumidor.

3. **Renuncia a Derechos**: Las cláusulas prohibidas a menudo intentan forzar al consumidor a renunciar a derechos que, por ley, no pueden ser renunciados.

> Esto puede incluir la renuncia a derechos legales, como el derecho a la protección contra prácticas comerciales desleales o el derecho a recibir una compensación en caso de incumplimiento contractual.

En el análisis de la protección de datos personales y los contratos de adhesión, se ha evidenciado la importancia de garantizar la equidad y la transparencia en las relaciones contractuales. De esta manera, la correlación entre la protección de datos personales y los contratos de adhesión subraya la necesidad de que los proveedores de servicios y entidades financieras cumplan con estándares rigurosos de transparencia, esto mediante la información debidamente proporcionada para que el titular de los datos personales consienta que se dé la recopilación y el tratamiento de los mismos , alineándose de esta forma con las obligaciones contractuales, garantizando que cualquier acuerdo establecido en un contrato de adhesión no contravenga los derechos de privacidad del consumidor. La correcta implementación de políticas de privacidad y la provisión de información adecuada y comprensible en los contratos son fundamentales para asegurar que los consumidores puedan tomar decisiones informadas y que sus datos sean gestionados de manera responsable para la protección de su privacidad.

2.3 ENTREVISTAS

Para abordar de manera integral la protección de datos en el ámbito financiero, resulta fundamental conocer las percepciones y experiencias tanto de los usuarios de servicios financieros como de las entidades regulatorias. Las entrevistas realizadas en este apartado se enfocan en dos perspectivas claves: la de los usuarios financieros, quienes enfrentan desafíos relacionados con la privacidad y el manejo de su información personal en instituciones bancarias, y la de la Superintendencia de Bancos, encargada de velar por el cumplimiento de normas de protección de datos y supervisar a las entidades financieras.

2.3.1 USUARIO FINANCIERO UNO

Se realizaron 5 preguntas entorno a la privacidad, protección de datos y cobro de obligaciones. Ahora bien, dentro de la primera pregunta se le cuestionó al usuario financiero ¿Qué entiende el por protección de datos en el contexto financiero? El mismo respondió que, la protección de datos personales en el contexto financiero se entiende que; una entidad se responsabiliza en resguardar y proteger la administración económica personal, ya sean en cuentas bancarias o tarjetas de crédito, a pesar de esto las entidades bancarias conocen nuestro manejo financiero y nos invitan a adquirir préstamos.

Como segunda pregunta se le cuestionó al informante si alguna vez su información personal ha sido utilizada sin su consentimiento. A lo que respondió de manera afirmativa ,estableciendo que las entidades financieras como bancos o cooperativas conocen nuestro manejo de cuentas y están constantemente insistiendo en que aceptemos préstamos o que nos endeudemos en promociones u ofertas que ellos patrocinan.

Como tercera pregunta, se le cuestionó al informante si considera que las entidades financieras brindan información clara sobre los derechos en cuanto a la protección de datos. La respuesta del informante uno fue negativa, estableciendo que de manera personal cree que los bancos o cooperativas son un sitio seguro donde se guarda dinero, sin embargo, no conoce los derechos con los que cuentan los usuarios financieros. Como cuarta pregunta, se le cuestionó si las políticas de privacidad de las entidades financieras son claras y accesibles. Por parte del informante uno la respuesta fue negativa, estableciendo que las entidades financieras son sitios para guardar dinero pero no tiene claro el tema de las políticas de privacidad.

La última pregunta ,versó netamente en el cobro de deudas, se le cuestionó si ha sentido que sus datos personales han sido revelados y si esto afecta a su privacidad. Esta respuesta fue afirmativa, el informante uno siente que sus datos si son revelados durante el proceso de cobro de deudas. Donde en ocasiones no solo el recibe llamadas sino sus contactos personales para comunicar sobre su situación financiera, el mismo considera que vulnera su privacidad, generando incomodidad respecto a que se revele su situación económica.

2.3.2 USUARIO FINANCIERO DOS

Se realizaron 5 preguntas entorno a la privacidad, protección de datos y cobro de obligaciones. Ahora bien, dentro de la primera pregunta se le cuestionó al usuario financiero ¿Qué entiende el por protección de datos en el contexto financiero? El informante dos respondió que se refiere al resguardo de la información personal sensible que manejan las entidades financieras. Los datos personales pueden incluir información como ingresos o deudas, como también nombre, número de identificación, y otros.

Como segunda pregunta se le cuestionó al informante dos si alguna vez su información personal ha sido utilizada sin su consentimiento, a lo que respondió de manera afirmativa estableciendo que en el contexto ecuatoriano siempre se utilizan los datos personales sin el consentimiento del titular, además agregó que, es de conocimiento público que las bases de datos son comercializadas al mejor postor.

Como tercera pregunta, se le cuestionó al informante si considera que las entidades financieras brindan información clara sobre los derechos en cuanto a la protección de datos. La respuesta del informante dos fue negativa, estableciendo que no hay información clara de sus derechos sobre sus datos personales.

Como cuarta pregunta, se le cuestionó si las políticas de privacidad de las entidades financieras son claras y accesibles. Por parte del informante uno la respuesta fue negativa.

La última pregunta, versó netamente en el cobro de deudas, se le cuestionó si ha sentido que sus datos personales han sido revelados y si esto afecta a su privacidad. Esta respuesta fue afirmativa, el informante dos estableció que durante el proceso de cobro, varias veces me llamaban a números de familiares. Me pareció que compartieron información personal sin mi consentimiento. Eso me afectó porque siento que mi privacidad fue vulnerada. No me sentí cómodo, y me dio la sensación de que todos sabían de mi situación financiera, lo cual es muy incómodo.

2.3.3 USUARIO FINANCIERO TRES

Se realizaron 5 preguntas entorno a la privacidad, protección de datos y cobro de obligaciones. Ahora bien, dentro de la primera pregunta se le cuestionó al usuario financiero ¿Qué entiende el por protección de datos en el contexto financiero? El informante tres respondió que la protección de datos versa en Salvaguardar la información sensible de los usuarios o cuentahabientes, que podrían ser usados con fines ilegales como la extorsión o la estafa.

Como segunda pregunta se le cuestionó al informante tres, si alguna vez su información personal ha sido utilizada sin su consentimiento, a lo que respondió de manera afirmativa, concordando así con el informante uno, en lo que respecta a las llamadas para ofrecer servicios financieros, sintiendo que esto ocurre sin su

consentimiento. El informante tres recalca que, existe entidades financieras a las cuales no ha solicitado servicios ni proporcionado sus datos personales, sin embargo, se contactan con él. Para el informante esto podría ser un indicador de la difusión no consentida de información sensible entre dichas entidades.

Como tercera pregunta, se le cuestionó al informante si considera que las entidades financieras brindan información clara sobre los derechos en cuanto a la protección de datos. La respuesta del informante tres fue negativa, estableciendo que no existe información específica sobre este tema, al menos en los medios convencionales.

Como cuarta pregunta, se le cuestionó si las políticas de privacidad de las entidades financieras son claras y accesibles. Por parte del informante tres, comentó que Se encuentra disponible esta información en los canales virtuales, pero no está muy difundida actualmente.

La última pregunta ,versó netamente en el cobro de deudas, se le cuestionó si ha sentido que sus datos personales han sido revelados y si esto afecta a su privacidad. El informante tres no está del todo seguro si sus datos fueron revelados, sin embargo, si ha recibido llamadas y mensajes de empresas de cobranza con información bastante específica sobre su deuda. Siendo un tema preocupante al no saber cuántas personas tienen acceso a esa información. Sintiendo que su privacidad está en riesgo, ya que no debería ser tan fácil para cualquier empresa acceder a los datos personales.

2.3.4 SUPERINTENDENCIA DE BANCOS

Se llevó a cabo una entrevista a un funcionario de la Superintendencia de Bancos con el objetivo de analizar cómo este organismo, como principal autoridad de control en el sector bancario, cumple su función de supervisar y proteger los datos personales de los usuarios financieros. De esta forma, la primera pregunta realizada gira en torno a como la Superintendencia de Bancos supervisa el uso y tratamiento de los datos personales de las entidades financieras. Así, este órgano enmarca su función de protección dentro del ámbito normativo regido por el Código Orgánico Monetario y Financiero; donde se establece la obligatoriedad de guardar confidencialidad de la información, así como la prohibición de comercialización de información y responsabilidades.

Dentro de las acciones de control que efectúa la Superintendencia de Bancos tiene supervisiones que se dan de manera extra situ e in situ; las cuales tienen el fin de velar

que las entidades sujetas a control cumplan debidamente con la normativa de su competencia, así como demitir sanciones en caso de que se evidencien incumplimientos. Actualmente las entidades del sistema financiero se encuentran ejecutando actualizaciones de los contratos de cuentas de ahorro, corrientes, tarjetas de crédito, etc, con el fin de adaptar el marco legal de la Ley Orgánica de Protección de Datos Personales.

En cuanto a la segunda pregunta, se le planteo al funcionario de la Superintendencia el cómo planea colaborar la mencionada institución con la nueva Superintendencia de Protección de Datos. Su respuesta se basa en el principio de colaboración establecido en el Código Orgánico Administrativo, de forma que las administraciones deben trabajar conjuntamente de manera coordinada, complementaria y prestándose auxilio, sin embargo, no se tiene un plan de acción en cuanto al trabajo conjunto que pueden realizar la Superintendencia de Bancos con la de Protección de Datos.

La tercera pregunta hace referencia al balance entre el acceso a datos financieros con la protección y el derecho a la privacidad de los usuarios. En este sentido, la respuesta otorgada se basa en la necesidad de que el organismo de control efectúe todas las acciones de control y actúen con las facultades que les permite la normativa vigente para precautelar que no se estén violentando los mismos y regular cualquier actividad improcedente. El funcionario hace referencia a que el sistema financiero nacional tiene la obligación de respetar el sigilo y la reserva que manda el artículo 353 del Código Orgánico Monetario y Financiero. Por otro lado, también hace referencia a la obligación que tienen tanto las personas naturales como jurídicas de acatar lo establecido en el artículo 355 del mismo código respecto a la no divulgación de la información que se les otorga.

Como última pregunta realizada al funcionario, se hizo referencia a los mecanismos que existen para que los usuarios financieros pueden reportar vulneraciones a la privacidad. En este sentido, en la actualidad existen canales virtuales y presenciales para los ingresos de quejas, consultas y reclamos y atención al usuario en general. A su vez, los usuarios pueden interactuar con la Superintendencia a través de redes sociales y los canales oficiales de la entidad.

CAPÍTULO 3

3.1 ANÁLISIS DE LA PROTECCIÓN DE DATOS

El tratamiento y protección de los datos personales en el sistema financiero es un tema de creciente importancia, especialmente en un contexto de mayor digitalización y uso intensivo de información por parte de las entidades financieras. Este acápite presenta un análisis comparativo de las percepciones de los usuarios financieros y el organismo de control que en el caso ecuatoriano es la Superintendencia de Bancos.

3.3.1 PERSPECTIVA USUARIOS FINANCIEROS

Las entrevistas realizadas a los usuarios financieros proporcionan una visión directa sobre sus preocupaciones, expectativas y experiencias en cuanto a la gestión de su información por parte de las instituciones financieras. Este enfoque permite identificar posibles brechas entre la normativa vigente y las prácticas percibidas por los usuarios.

De esta forma, en la primera pregunta se consulta a los informantes sobre su comprensión de la definición de datos personales. Si bien cada uno de los entrevistados tienen pleno entendimiento sobre qué comprenden los datos personales dentro del contexto financiero, es importante resaltar un punto trascendental. Los tres entrevistados mencionan que las entidades financieras son las encargadas del "resguardo de la información personal sensible", "se responsabiliza en resguardar y proteger la administración económica personal" y "Salvaguardar la información sensible de los usuarios o cuentahabientes".

Así, los entrevistados demuestran un claro entendimiento de que las entidades financieras, al asumir el rol de responsables del tratamiento de datos personales, no solo deciden sobre la finalidad y los métodos de uso de esta información, sino que también adquieren un compromiso jurídico y ético con la protección de la privacidad de los usuarios. Esta responsabilidad implica que las instituciones financieras deben implementar medidas de seguridad adecuadas para evitar accesos no autorizados, pérdidas o alteraciones de los datos.

El reconocimiento de esta responsabilidad no es algo reciente o nuevo de la ley de protección de datos, sino que responde a la dinámica establecida entre los usuarios y las

instituciones financieras, donde estas últimas, al tener acceso a información sensible sobre la situación económica de las personas, como ingresos, deudas y patrones de consumo, se convierten en depositarias de confianza. Esta confianza se traduce en una expectativa legítima de que las entidades actúen con diligencia y prudencia en la protección de dichos datos, evitando su uso indebido o la vulneración de la privacidad de los usuarios.

Además, esta conciencia por parte de los informantes también pone de relieve un aspecto fundamental del marco regulatorio, es decir, la necesidad de un equilibrio entre el acceso a la información para la gestión eficiente de los servicios financieros y la protección de los derechos de los usuarios. Entendiéndose que las prácticas de las instituciones financieras deben alinearse con principios de transparencia y legalidad, garantizando que los datos sean utilizados exclusivamente para los fines declarados y consentidos.

Ahora bien, dentro de la segunda pregunta se les consultó a los informantes si alguna vez han sentido que su información financiera ha sido utilizada sin su consentimiento. Para el informante dos esto resulta una práctica usual dentro del contexto ecuatoriano, sin embargo, la respuesta otorgada por los entrevistados 1 y 3 resulta particularmente interesante, ya que señalan que sus datos personales han sido utilizados sin su consentimiento para la comercialización de productos dentro del sistema bancario.

La respuesta proporcionada guarda relación con la tercera y cuarta pregunta planteada, ya que en la tercera se hace referencia a si los usuarios financieros reciben información clara sobre los derechos que tienen respecto a sus datos personales. Dentro de esta pregunta, los tres informantes coinciden que las instituciones financieras no otorgan información clara sobre los derechos que tienen respecto a sus datos personales, estableciendo que “no se conoce los derechos que contamos como usuarios” o “No existe información específica sobre este tema, al menos en los medios convencionales”. Informar a los usuarios financieros sobre sus derechos en relación con la protección de sus datos personales es una obligación fundamental de las instituciones financieras, para que de esta forma el usuario autorice el tratamiento de sus datos personales, es necesario que exista lo que se conoce como consentimiento informado.

¿Qué comprende el consentimiento informado? En la Ley Orgánica de Protección de Datos Personales en el artículo 8 (Ley Orgánica de Protección de Datos, 2024),

establece cuatro puntos importantes en los cuales se debe basar el Consentimiento. El primero es que este debe ser libre, es decir, debe otorgarse de manera voluntaria, sin coerción, error, dolo ni ningún otro vicio que pueda comprometer la voluntad del titular de los datos. En consecuencia, el consentimiento es considerado válido únicamente cuando se proporciona de forma consciente y sin influencias indebidas. Como segundo aspecto, para que el titular de los datos personales otorgue su consentimiento para el tratamiento de su información, este debe ser específico, es decir, el tratamiento de los datos debe ser claramente definido, establecer el tiempo de conservación; que en el contexto ecuatoriano, las instituciones financieras pueden almacenar los datos personales por un período máximo de seis años a partir de la fecha de vencimiento de la obligación, de acuerdo con el Artículo 358 del Código Orgánico Monetario Y Financiero, Libro I, refiriéndose así a la información de riesgo crediticio. Además, los reportes de información crediticia solo deben incluir las operaciones de los tres últimos años previos a la fecha de emisión del reporte. Como último , deben ser limitados a fines concretos.

El tercer requisito es el consentimiento informado. La expresión informado implica que el titular de los datos debe recibir información clara y comprensible sobre cómo se utilizarán sus datos, incluyendo los fines del tratamiento, los destinatarios de la información, y sus derechos asociados. Esto garantiza el cumplimiento del principio de transparencia, que exige que las instituciones financieras actúen de manera clara y accesible. Al proporcionar esta información, se efectiviza el derecho a la transparencia, permitiendo a los usuarios tomar decisiones informadas sobre el manejo de su información personal.

Como último requisito ,el consentimiento debe ser inequívoco, es decir, que la autorización proporcionada por el titular de los datos debe ser clara y sin ambigüedades, de modo que no haya lugar a interpretaciones erróneas sobre el alcance del consentimiento. Esto es fundamental para asegurar que el titular comprenda exactamente qué datos se están tratando, con qué fines y quién tendrá acceso a ellos. La claridad en la autorización protege los derechos del titular y fortalece la confianza en las instituciones que manejan su información personal.

Ahora bien, dentro de los derechos que los usuarios financieros gozan son:

- Derecho al acceso: Los titulares pueden solicitar información sobre los datos personales que una entidad tiene sobre ellos y cómo se están utilizando. El propósito de esta facultad es garantizar que el titular de los datos esté informado

sobre qué datos se están procesando y, por lo tanto, sobre las posibles consecuencias que podrían surgir del tratamiento de dicha información. (Aponte, 2007).

- Derecho de Rectificación: Tienen el derecho de solicitar la corrección de datos personales inexactos, incompletos o desactualizados. Es decir, implica la capacidad del titular de los datos de requerir al responsable del tratamiento que respete el principio de calidad, corrigiendo cualquier error o completando la información faltante, de manera que el tratamiento refleje de forma precisa y veraz de la realidad.

- Derecho de Cancelación: Los titulares pueden pedir la eliminación de sus datos personales cuando ya no sean necesarios para los fines para los cuales fueron recopilados o si se ha ejercido un uso indebido. Facultando al titular de los datos a solicitar al responsable del tratamiento que cumpla con el principio de calidad, rectificando cualquier inexactitud o agregando la información necesaria, de modo que el tratamiento de los datos represente fielmente la realidad (Aponte, 2007).

- Derecho de Oposición: Pueden oponerse al tratamiento de sus datos personales en ciertas circunstancias, como cuando se utilizan con fines de mercadeo.

Ahora bien, una vez analizado la importancia del consentimiento informado de los usuarios financieros es importante retomar lo manifestado por los informantes respecto a las llamadas por parte de los bancos para ofrecer servicios.

Por situación de confidencialidad, para realizar un análisis sobre el consentimiento que se les otorga a las entidades financieras se hará referencia a la institución financiera B. Dentro de los contratos de esta institución financiera, en el apartado sobre el tratamiento de los datos personales, se establece que se le autoriza a dicha institución para realizar llamadas ofertando los distintos productos que la misma ofrece. Es decir, que el titular de los datos una vez que firme un contrato con la institución financiera ,autoriza para que este tipo de situaciones sucedan.

Desde el punto de vista analítico, por un lado el banco está informando que si llega a ver la relación contractual usuario/entidad, se les autoriza para ofertar sus productos. Cumpliendo así con la obligación de informar la finalidad para la cual sus datos son tratados. Sin embargo, esta situación puede caer en una relación abusiva, pues las entidades financieras pueden aprovechar que se dio el consentimiento para realizar estas prácticas ,y, por querer ofertar sus productos caen en el acoso. Siendo esto según

> la Codificación de la Superintendencia de Bancos Libro Primero Tomo IV, como cualquier forma de hostigamiento, ya sea directa o indirectamente, llevada a cabo por entidades financieras, ya sean públicas o privadas, así como por organismos del sistema de seguridad social, hacia los consumidores financieros, ya sea por medio de terceros o de manera propia (Codificación Superintendencia De Bancos, Libro Primero Tomo IV, 2024).

Ahora bien, tras haber analizado la importancia de informar a los usuarios financieros sobre sus derechos, es necesario examinar este aspecto en relación con la pregunta cuatro planteada a los informantes. Esta pregunta se refiere al conocimiento de las políticas de privacidad implementadas por las entidades financieras, y, si estas son claras y accesibles. Los tres entrevistados coincidieron en que dichas políticas no están fácilmente al alcance de los usuarios financieros.

Pero ¿Cuál es la importancia de estas políticas? Para comprender qué son, es necesario referirse a lo dispuesto por la normativa, la cual establece que son las directrices y procedimientos internos, documentados por escrito y aplicados por las entidades supervisadas, con el fin de asegurar la protección de la privacidad de la información confidencial de los clientes. (Codificación Superintendencia De Bancos Libro Primero Tomo IV, 2024).

La política de privacidad es un elemento clave para el cumplimiento de las normativas de protección de datos personales. Esta incluye, entre otros aspectos, los tipos de datos recopilados, la finalidad del tratamiento, la base legal que lo sustenta, la posibilidad de compartir los datos con terceros y el proceso correspondiente, los derechos del titular de los datos, y las medidas de seguridad [16] implementadas para su protección.

En conclusión, las políticas de privacidad son esenciales para proteger la información confidencial de los usuarios financieros, garantizando que las entidades financieras cumplan con las normativas de protección de datos personales. Sin embargo, como se desprende de la percepción de los entrevistados, existe una falta de accesibilidad y claridad en la información proporcionada por estas políticas, lo que dificulta que los usuarios comprendan cómo se gestionan sus datos. Por lo tanto, es crucial que las entidades financieras cumplan con la obligación de hacer que sus políticas de privacidad sean más claras, comprensibles y accesibles, asegurando así la confianza de los usuarios

---

[16] Información tomada de la Pagina web: https://lawwwing.com/

y el cumplimiento efectivo de sus derechos en relación con la protección de su información personal.

Como última pregunta que se realizó a los entrevistados, se estableció si durante el proceso de cobro de deudas han sentido que sus datos personales han sido revelados, y, como esto afecta a su privacidad. La respuesta de los tres informantes fue afirmativa, haciendo referencia "En varias ocasiones, los cobradores han llamado a mis contactos personales para comunicar mi situación financiera, algo que considero una violación a mi privacidad. Me ha generado mucha incomodidad, ya que siento que la información sobre mi situación económica es algo privado y no debería ser compartida con terceros sin mi consentimiento", "Me pareció que compartieron información personal sin mi consentimiento", "No estoy seguro si mis datos fueron revelados, pero sí recibí llamadas y mensajes de empresas de cobranza con información bastante específica sobre mi deuda."

Una vez expuesto la opinión de los informantes, se debe partir de lo manifestado por el artículo 18 del reglamento a la Ley Orgánica de Protección de datos que hace referencia a los datos crediticios. Este artículo permite el tratamiento de datos personales con el objetivo de informar sobre el cumplimiento o incumplimiento de obligaciones comerciales o crediticias. Esto significa que los datos relacionados con el historial crediticio de una persona pueden ser recolectados, procesados y utilizados de manera legítima por entidades autorizadas, siempre que este procesamiento esté orientado a evaluar la capacidad o comportamiento crediticio de los individuos o empresas. Aquí se incluye información tanto positiva como negativa de las obligaciones crediticias.

¿Como las entidades tienen el conocimiento de los datos crediticios de las personas? Pues bien, dentro del contexto financiero existe lo que se conoce como Buró de crédito, mismo que actúa como una carta de presentación financiera, proporcionando a bancos e instituciones un informe detallado sobre como los usuarios gestionan sus finanzas a través de su historial crediticio (Equifax, 2024). De esta forma, el buró de crédito actúa como intermediario entre las entidades financieras y los individuos; recolectando información sobre el historial de crédito de una persona o empresa, como el cumplimiento de pagos, saldos de deudas y otros comportamientos crediticios.

A través del buró de crédito, las entidades financieras pueden evaluar el nivel de cumplimiento de los usuarios respecto al pago de sus obligaciones crediticias. Este

registro incluye tanto información negativa como positiva, proporcionando una visión completa del comportamiento crediticio de cada individuo o empresa.

Esta información es fundamental para las instituciones financieras al momento de decidir la concesión de un crédito, debido a que al analizar los datos proporcionados por el buró, pueden determinar con mayor precisión el nivel de responsabilidad financiera del solicitante. De este modo, no solo se protege a las entidades de asumir riesgos excesivos, sino que también se garantiza que los usuarios con un historial crediticio favorable tengan acceso a mejores condiciones crediticias. En este sentido, el buró de crédito no solo actúa como un filtro para prevenir el sobreendeudamiento, sino que también fomenta la responsabilidad financiera y la transparencia en las relaciones crediticias. Además, este mecanismo contribuye a la estabilidad del sistema financiero al proporcionar una base de datos que permite evaluar el riesgo crediticio de forma objetiva, reduciendo la probabilidad de impagos y mejorando la asignación de recursos financieros en la economía.

Por otro lado, están las compañías auxiliares que, como se analizó antes están reguladas en la Codificación de la Superintendencia de Bancos. Siendo estás las encargadas del cobro de cartera de las entidades financieras, están igualmente obligadas a resguardar las bases de datos que se les ha sido conferidas. El artículo 23[17] de la Codificación de la Superintendencia De Bancos Libro Primero Tomo I, impone a las compañías auxiliares la responsabilidad de garantizar que la información proporcionada por las entidades financieras sea protegida de manera íntegra y segura. Esto implica la adopción de medidas técnicas y organizativas para evitar filtraciones, accesos no autorizados o manipulación de datos.

Las compañías auxiliares, como actores clave en la gestión de la cartera de clientes de las entidades financieras, adquieren un rol importante en el manejo de datos personales.

---

[17] Art. 23.- Las Compañías de Servicios Auxiliares deberán resguardar las bases de datos y la información de datos no públicos proporcionada por la entidad financiera contratante de manera íntegra y segura, entiéndase a ésta como la información relacionada con el suministro de productos o servicios financieros de consumos, como información fotográfica y biométrica. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad, siempre que su uso haya sido debidamente autorizado por el titular, esto de conformidad con lo dispuesto en el Código Orgánico Monetario Financiero y la Ley de Comercio Electrónico y Mensajes de Datos. (CODIFICACIÓN SUPERINTENDENCIA DE BANCOS, LIBRO PRIMERO TOMO I, 2024).

Según el Artículo 23 del Código Orgánico Monetario y Financiero, estas compañías están obligadas a resguardar de manera íntegra y segura las bases de datos que les han sido confiadas por las entidades financieras.

Es decir, aquí es donde surge la necesidad de implementar políticas de privacidad específicas para regular la relación entre las entidades financieras y las compañías auxiliares. Si bien las políticas de privacidad establecidas por las entidades f financieras son esenciales, su aplicación extensiva a las relaciones con terceros, como las compañías auxiliares, garantiza que el tratamiento de los datos cumpla con los mismos estándares de protección, sin importar quién los gestione. Para garantizar un correcto manejo de los datos personales, las políticas de privacidad no pueden limitarse a la operación interna de las entidades financieras. Estas deben ser implementadas de manera vinculante en los contratos y acuerdos con las compañías auxiliares. Esto implica que las entidades financieras deben incluir cláusulas específicas sobre el tratamiento de datos, asegurando que las compañías auxiliares no solo resguarden la información de manera segura, sino que también respeten los derechos fundamentales de los titulares de los datos, como la privacidad y la confidencialidad.

Asimismo, el Reglamento de la Ley Orgánica de Protección de Datos Personales establece las obligaciones que tienen los terceros al momento de transferir los datos de los titulares a otras entidades. Este proceso debe fundamentarse en el consentimiento informado del titular. Como se analizó anteriormente, dentro de los contratos de adhesión suscritos por las instituciones financieras, se incluye una cláusula que estipula la posibilidad de que estas entidades cedan a terceros los datos personales de sus clientes.

Pero ¿Qué implica esto? Dentro del mismo reglamento [18] se dispone que cuando se realice la transferencia de datos personales a terceros se deben cumplir con dos supuestos, el primero es que se cumplan con los fines directamente relacionados con las funciones legitimas del responsable, haciendo referencia a la legitimidad de las funciones del responsable del tratamiento (quien determina los fines y medios del tratamiento) y del tercero destinatario (quien recibe y trata los datos). Este enfoque resalta dos puntos importantes:

[18] Art. 22 .- Supuestos para la transferencia de datos a terceros.- La transferencia o comunicación de datos personales a terceros se podrá realizar siempre que concurran los siguientes supuestos: 1. Para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del tercero destinatario, en cuyo caso el destinatario se obliga a cumplir con la normativa de protección de datos; y, 2. Cuando se cuente con el consentimiento previo del titular, el cual puede ser revocado en cualquier momento. (Reglamento de protección de datos [RPD], 2024), art. 22).

1. **Legitimidad:** los fines para los cuales se tratan los datos personales deben estar alineados con funciones legítimas, lo que implica que no deben ser arbitrarios o abusivos. Por ejemplo, en el ámbito financiero, una entidad puede compartir datos personales con un tercero para fines de gestión de crédito o cobranza, siempre que estas actividades estén enmarcadas en su objeto social y sean necesarias para el cumplimiento de sus obligaciones contractuales.

2. **Propósito específico:** El tratamiento de datos debe estar dirigido a cumplir con finalidades claramente definidas y comunicadas a los titulares de los datos. Esto refuerza la idea de que los datos no deben ser utilizados para fines distintos a los originalmente previstos, a menos que se obtenga un nuevo consentimiento del titular.

Y el segundo supuesto como se analizó antes es tener el consentimiento informado del titular de los datos personales.

En el contexto del proceso de cobro de obligaciones, las compañías auxiliares de cobranza, en principio, ejercen su facultad de cobro, lo que incluye la posibilidad de comunicarse con el deudor y sus garantes. Sin embargo, como se observó en las entrevistas, el problema radica en que no solo se comunican con el deudor y sus garantes, sino que también realizan llamadas a terceros que no fueron pactados para llevar a cabo este proceso de cobranza. La vulneración del derecho a la privacidad no solo afecta al deudor al momento de revelar información relacionada con su obligación, sino que también impacta el derecho a la privacidad de los terceros a quienes se les realiza la llamada. En principio, el deudor solo pacta el tratamiento de sus datos y los de sus garantes en el contexto de esta obligación. Sin embargo, al contactar a terceros que no están involucrados en el acuerdo, se está accediendo a información de personas que no han otorgado su consentimiento para que sus datos sean tratados.

Esto otorga no solo al deudor la facultad de denunciar este tipo de abusos, sino también a los terceros que son contactados, ya que estos últimos no han proporcionado su consentimiento para el tratamiento de sus datos. Esto plantea la inquietud: ¿cómo se obtuvo la información de estos terceros si no se les autorizó?

En el contexto ecuatoriano, la venta de datos personales se ha convertido en una práctica común, lo que ha llevado a la difusión de información sin el consentimiento de los titulares. Esta situación impide a los individuos ejercer sus derechos de rectificación,

cancelación y oposición. En este contexto, es fundamental destacar que las políticas de privacidad no solo deben ser implementadas por las entidades financieras, sino que son obligatorias para cualquier entidad o individuo que maneje datos personales. Esto garantiza que se respeten los derechos de los titulares y se establezcan medidas adecuadas para la protección de la información, promoviendo así un manejo ético y responsable de los datos.

3.3.2 PERSPECTIVA SUPERINTENDENCIA DE BANCOS

La perspectiva de la Superintendencia de Bancos es crucial para entender las políticas y prácticas implementadas en el sector financiero en torno a la protección de datos personales. A través del análisis de esta entrevista, se busca obtener un panorama detallado de las medidas adoptadas por la Superintendencia para garantizar el cumplimiento de las normas de confidencialidad y privacidad de la información de los usuarios.

De esta forma, se debe partir desde el punto principal de esta investigación, es decir, como la Superintendencia de Bancos supervisa el uso y tratamiento de los datos de sus entidades controladas. El funcionario de este organismo de control hace referencia a las funciones que determina el artículo 62[19] del Código Orgánico Monetario y Financiero, dentro del cual se dispone las funciones de está superintendencia; que para esta investigación se enmarcan en los numerales 16 y 17.

Por un lado, se puede desglosar el numeral 16 en tres aspectos importantes respecto a las actividades de que realiza esta superintendencia. El primero versa sobre la protección de datos en sí, este punto implica un mandato directo a la entidad de control para salvaguardar los derechos e intereses de los usuarios y clientes. Siendo importante resaltar que estos derechos abarcan la transparencia, la protección de datos personales y la confidencialidad, áreas que juegan un rol crucial en la confianza en el sistema

[19] Art. 62.- Funciones. La Superintendencia de Bancos tiene las siguientes funciones:
16. Proteger los derechos de los usuarios y/o clientes del sistema financiero y resolver las controversias en el ámbito administrativo que se generen con las entidades bajo su control, para lo cual deberá solicitar o practicar de oficio, según sea el caso, las acciones de control necesarias para su esclarecimiento, conforme las disposiciones normativas que deberá emitir para el efecto;
17. Establecer las cláusulas obligatorias y las prohibiciones de los contratos cuyo objeto sea la prestación de servicios financieros. (Código Orgánico Monetario y Financiero [COMF], 2014, art. 62).

financiero. Aquí se refuerza la importancia de los derechos de privacidad y de protección de datos personales. La entidad de control asume el rol de velar que las instituciones financieras cumplan con las normativas que protegen los datos y la información sensible de los clientes. Esto está en correlación con el marco legal, tanto en la Constitución, que establece el derecho a la intimidad y la privacidad, como en la Ley Orgánica de Protección de Datos Personales.

El segundo punto versa sobre la resolución de controversias dentro del ámbito administrativo. En este aspecto, la entidad no solo actúa como supervisor, sino también como mediador y fiscalizador, investigando de oficio o a petición de parte, en caso de controversias sobre el tratamiento de datos personales o la confidencialidad de la información de los clientes. Siendo indispensable que al momento de resolver controversias, la entidad de control debe actuar conforme a procedimientos administrativos y respetando el debido proceso, asegurando imparcialidad y celeridad. Como último punto, hace referencia a las acciones y el control normativo que la Superintendencia de bancos debe asegurar, siendo necesario que la misma examine e implemente las herramientas legales y los procedimientos , qué como superintendencia debe emplear para hacer cumplir los derechos de los usuarios en caso de incumplimiento o malas prácticas de parte de las entidades financieras.

Otorgándole una facultad de actuar de oficio, ya que permite a la entidad intervenir incluso sin solicitud de los afectados. La función de control incluye inspecciones, auditorías o cualquier otra acción que permita garantizar el cumplimiento de las normativas aplicables. Esto muestra un enfoque proactivo en el control y fiscalización. Así, esta institución tiene además la facultad de emitir sus codificaciones en su ámbito de regulación y control, porque se debe entender que el principal objetivo de esta institución versa en ser una entidad técnica y autónoma encargada de supervisar y controlar las instituciones de los sectores público y privado en el sistema financiero, así como el sistema nacional de seguridad social, con el objetivo de garantizar su seguridad, estabilidad, solidez y transparencia. De esta manera, se protege el ahorro del público, los pensionistas, afiliados y contribuyentes, así como el interés general de los ciudadanos que acceden a productos y servicios financieros, y reciben prestaciones de calidad (Superintendencia de Bancos, 2024).

Teniendo así un rol de supervisión y control, donde debe asegurar que las entidades financieras respeten y protejan la información personal y financiera de sus usuarios. Esto involucra que el tratamiento de los datos personales sea realizado de acuerdo con la normativa vigente sobre privacidad, resguardando los derechos constitucionales de los usuarios y protegiendo su información contra usos indebidos o vulneraciones de confidencialidad. De esta forma, se encarga de mantener en equilibrio la relación entre las entidades financieras y sus usuarios, que como se analizó con anterioridad, esto se puede ver afectado con los contratos de adhesión que estas instituciones manejan.

Esto se conecta con el numeral 17 que hace referencia el funcionario de esta superintendencia. Dentro del cual se manifiesta la obligación de establecer cláusulas y prohibiciones específicas en los contratos de servicios financieros; teniendo un rol central en la protección de los derechos de los usuarios, particularmente en lo que respecta a la privacidad y al manejo de datos personales. Como se analizó con anterioridad, esto hace referencia al contrato de adhesión que manejan las instituciones bancarias al momento de ofrecer sus servicios. Donde al tener la voluntad de una de las partes al momento de realizarlo, esto puede afectar a la otra parte que tiene la opción de adherirse o no al contrato.

La función de la Superintendencia de Bancos para equilibrar la relación contractual entre usuarios y entidades financieras tiene un papel crucial en la protección de los derechos de los consumidores, especialmente mediante la prevención de cláusulas abusivas y prohibidas en contratos bancarios. Que por un lado, las primeras cláusulas colocan al usuario en una clara desventaja frente a la entidad financiera, ya que imponen obligaciones desproporcionadas o limitan injustamente sus derechos. En este sentido además, la Ley Orgánica de Defensa del Consumidor en Ecuador prohíbe expresamente tales cláusulas abusivas, lo que se alinea con la supervisión que la Superintendencia de Bancos debe realizar. En los contratos de adhesión, donde el cliente generalmente no tiene la posibilidad de negociar los términos, las cláusulas abusivas son especialmente problemáticas, ya que pueden incluir términos como cargos excesivos, modificaciones unilaterales del contrato, o limitaciones al derecho de reclamar.

Y por el otro lado, las segundas cláusulas tienen un carácter intrínsecamente injusto o ilegal. Como ejemplo enfocado a los datos personales , estos contratos no pueden

incluir disposiciones que vulneren derechos fundamentales, como el derecho a la privacidad, o que permitan el tratamiento o divulgación indebida de los datos personales de los usuarios. La Superintendencia de Bancos, al supervisar estos contratos, debe asegurar que no se incluyan disposiciones que otorguen a las entidades financieras el derecho a utilizar los datos de los clientes más allá de lo permitido por la ley, o que limiten injustamente la responsabilidad de la institución frente a una vulneración de la información personal.

Así pues, la Superintendencia de Bancos, como entidad de control, es clave para mantener el equilibrio entre los derechos del usuario y las prerrogativas de las entidades financieras. La combinación de normativas internas de la Superintendencia con otras leyes garantiza que los contratos de servicios financieros no solo cumplan con las normas de transparencia y equidad, sino que también ofrezcan un nivel de protección adecuado respecto a la confidencialidad y tratamiento de los datos personales de los usuarios. Esto en referencia a las funciones que esta institución debe cumplir.

Además, cabe mencionar que el funcionario público a quien se le realizó la entrevista también agrega que existe una disposición general respecto a la protección de datos del Código Orgánico Monetario y Financiero dentro del artículo 352[20], el cual se dispone que los datos personales de los usuarios del sistema financiero están protegidos, lo que implica que estas entidades tienen la obligación legal de implementar medidas que garanticen la seguridad y confidencialidad de la información que gestionan. Esto está alineado con los principios de privacidad y confidencialidad recogidos en la Constitución de la República del Ecuador y en la Ley Orgánica de Protección de Datos Personales. La norma exige que los datos sean manejados de forma tal que se minimicen los riesgos de exposición indebida, robo o acceso no autorizado.

Conectando esta idea con lo previamente analizado solo el titular de los datos o un autorizado puede acceder a la información. Esto destaca la importancia del consentimiento explícito y fundamenta el derecho de los usuarios sobre sus propios datos, protegiéndolos frente a accesos o transferencias no autorizadas. Además, se debe agregar

[20] Art. 352.- Protección de la información. Los datos de carácter personal de los usuarios del sistema financiero nacional que reposan en las entidades de dicho sistema y su acceso están protegidos, y solo podrán ser entregados a su titular o a quien éste autorice o por disposición de este Código. (Código Orgánico Monetario y Financiero [COMF], 2014, art. 352).

el artículo 360 del mismo código. En el cual se establece la prohibición de la comercialización y la alteración de la información que haga referencia al historial crediticio de los usuarios.

Pero ¿Cómo la Superintendencia de Bancos garantiza el cumplimiento de estas disposiciones? El funcionario de esta institución explica que se realizan "supervisiones extra situ e in situ las cuales tienen el fin de velar que las entidades sujetas a control cumplan debidamente con la normativa de su competencia, así como de emitir sanciones en caso de que se evidencien incumplimientos". Respecto a estas supervisiones se debe entender que las mismas se realizan de la siguiente manera:

- Supervisión Extra Situ: Se refiere a la supervisión que se realiza de manera remota, utilizando información que las entidades financieras deben reportar periódicamente. Esto incluye el análisis de informes financieros, estados de cuenta, revisión y aprobación de contratos emitidos por las instituciones, etc. Esto con el objetivo de evaluar la situación financiera y operativa de las entidades, detectar irregularidades, riesgos o problemas potenciales en la gestión de las entidades y monitorear el cumplimiento de normativas y regulaciones vigentes.

- Supervisión In Situ: Esta forma de supervisión implica visitas físicas a las oficinas y sucursales de las entidades financieras. La Superintendencia realiza inspecciones para evaluar directamente el funcionamiento y la gestión de las instituciones. Esto con el objetivo de realizar un examen detallado de la situación operativa, administrativa y financiera de las entidades, Comprobar la veracidad de la información reportada en los informes extra situ e identificar problemas o deficiencias en los procesos internos y el cumplimiento de la normativa.

La combinación de estas dos formas de supervisión permite a la Superintendencia de Bancos garantizar la seguridad, estabilidad, solidez y transparencia del sistema financiero ecuatoriano. A través de la supervisión extra situ, se pueden identificar tendencias o problemas emergentes, mientras que la supervisión in situ proporciona una evaluación más profunda y directa de cómo se gestionan las instituciones y si cumplen con las normativas sobre la protección de datos y derechos de los usuarios.

Cabe agregar que, a más de estás supervisiones que realiza la Superintendencia de Bancos. Es importante resaltar que en la actualidad, las entidades financieras están

realizando actualizaciones del contrato sobre cuentas de ahorro, corrientes, tarjetas de crédito, etc. Si bien esto es importante ¿Cuáles son las razones que han llevado al sistema financiero a implementar estas actuaciones recientemente, y porque no se llevaron a cabo en etapas anteriores? Como es de conocimiento, la Ley Orgánica de Protección de Datos Personales fue promulgada en el año 2021, sin embargo, la Superintendencia de Datos Personales fue constituida recién en el año 2024.

Es importante señalar que la Superintendencia de Protección de Datos Personales es la entidad encargada de la potestad sancionadora respecto al uso indebido de datos personales, conforme lo establece la Ley Orgánica de Protección de Datos Personales. Esta normativa contempla sanciones específicas por el mal uso de la información. Sin embargo, desde su promulgación en el año 2021, no existía un ente regulador efectivo, dado que la Superintendencia de Protección de Datos Personales fue constituida recientemente en el año 2024.

La reciente constitución de esta superintendencia ha generado un vacío en la aplicación de la normativa, ya que, aunque se ha establecido la entidad, aún no ha comenzado a cumplir plenamente sus funciones. Esto ha dado lugar a una falta de cumplimiento de la Ley Orgánica de Protección de Datos Personales, lo que limita la protección efectiva de los derechos de los usuarios en relación con sus datos personales.

Una vez realizado este análisis, la segunda pregunta que se le planteó al funcionario de la Superintendencia de Bancos fue como la misma planea trabajar con la recientemente constituida Superintendencia de Protección de datos. La respuesta dada fue en el ámbito que establece la Constitución de la República del Ecuador en su artículo 28, el cual hace referencia al principio de colaboración que rige sobre las administraciones públicas en los cuales se basa en el auxilio muto, coordinado y complementario. No obstante, esto no es suficiente para establecer un plan de acción efectivo entre la Superintendencia de Bancos y la Superintendencia de Protección de Datos Personales. Como es de conocimiento público, el escaso control por parte del estado ecuatoriano ha permitido que los datos personales de sus habitantes sean difundidos sin su consentimiento. A pesar de que existe una normativa sobre la protección de datos desde 2021, esta no ha sido suficiente, ya que es imprescindible que la Superintendencia de Protección de Datos ejerza su función para garantizar una protección efectiva.

En este sentido, es importante destacar que los datos bancarios son actualmente los que más se distribuyen, lo que afecta gravemente la privacidad de los usuarios financieros. Por lo tanto, es fundamental que ambas superintendencias colaboren de manera conjunta. Si bien los datos han sido difundidos, es necesario comenzar a limitar su uso y tratamiento a través de las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales. La difusión de datos no exime el derecho a la privacidad e intimidad, derecho que el Estado tiene la obligación de garantizar y hacer efectivo.

En esta línea, la tercera pregunta realizada al funcionario público de la Superintendencia de Bancos se destaca en el balance que la Superintendencia debe mantener en cuanto al acceso a los datos financieros, equilibrando esta necesidad con la protección y el derecho a la privacidad de los usuarios. En la respuesta que fue otorgada se estableció la obligación que tiene los organismos de control de efectuar las acciones de control y actuar con las facultades que les permite la normativa vigente para precautelar que no se estén violentando los mismos y regular cualquier actividad improcedente.

Haciendo respetar lo que anteriormente se analizó como *sigilo bancario*, es decir, esta obligación impuesta a las entidades financieras de no proporcionar la información que haga referencia a la información bancaria de los usuarios financieros. Es imperativo que los derechos de los usuarios sean respetados en todas las dimensiones de la interacción con las entidades financieras. Esto incluye no solo el derecho a la privacidad y la confidencialidad de sus datos, sino también el derecho a ser informados sobre el uso de su información personal y a recibir un tratamiento justo y equitativo.

De esta forma, por un lado se tiene al artículo 353 del Código Orgánico Monetario y Financiero. Este artículo establece el principio de sigilo y reserva en las operaciones del sistema financiero. Las entidades deben proteger la información de sus usuarios, asegurando que los datos personales no sean divulgados sin el consentimiento correspondiente. Esto es crucial para mantener la confianza de los usuarios en el sistema financiero, y, por el otro lado, se tiene el artículo 355 del código antes mencionado, donde refuerza la obligación de no divulgar información sobre los usuarios, imponiendo sanciones y responsabilidad penal a quienes infrinjan esta disposición.

Es decir, por un lado el Código Orgánico Integral penal en el artículo 180[21] numeral 1, el cual dispone una pena de 1 a 3 años aquellas personas que revelen información protegida cuando este contenida expresamente en una cláusula de reserva, y, por el otro, el mismo Código Orgánico Monetario y Financiero en el artículo 272[22] dispone una sanción pecuniaria de 30 salarios básico-unificados a las personas naturales o jurídicas que divulguen ya sea de forma total o parcial la información sujeta al sigilo.

¿Pero cómo saber quién fue el que divulgó la información? Determinar quién ha divulgado información confidencial se ha vuelto cada vez más complejo. En el ámbito financiero, las instituciones cuentan con la facultad de vender sus carteras a compañías auxiliares. Sin embargo, no existe un mecanismo eficaz para controlar el uso posterior que estas empresas hacen de los datos personales. Esto genera un riesgo, ya que las compañías auxiliares podrían, a su vez, revender las bases de datos que les fueron proporcionadas, creando una cadena en la cual se pierde el rastro del origen de la divulgación. Esta falta de trazabilidad compromete la seguridad de los datos personales y dificulta la identificación de la fuente original de la filtración, lo cual es particularmente preocupante desde la perspectiva de la protección de datos y la confidencialidad en el sector financiero.

No obstante, es posible sancionar a quien está manejando los datos personales en caso de uso indebido o tratamiento sin el consentimiento del titular. Si bien las entidades financieras pueden vender su cartera y, con ella, su base de datos, al realizar esta transferencia están obligadas a tener una política de privacidad de datos. Esta política no solo debe aplicarse a sus usuarios financieros, sino también extenderse a las compañías a las cuales se transfieren los datos personales, estableciendo claramente cómo deben manejar dicha información. Es importante destacar que las bases de datos solo pueden utilizarse para los fines acordados originalmente entre el usuario financiero y la entidad, como la gestión de cobro de deudas y la identificación de posibles garantes. Las compañías auxiliares están limitadas a operar únicamente dentro de este ámbito, ya que

[21] Art. 180.- Difusión de información de circulación restringida. - La persona que difunda información de circulación restringida será sancionada con pena privativa de libertad de uno a tres años. Es información de circulación restringida: 1. La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley. (Código Orgánico Integral Penal [COIP], 2024, art. 180). [22] Art. 272.- Sanción por divulgación de información. Las personas naturales o jurídicas que divulguen, en todo o en parte, información sometida a sigilo o reserva, serán sancionadas con una multa de treinta y cinco salarios básicos unificados, sin perjuicio de la responsabilidad penal que corresponda. (Código Orgánico Monetario y Financiero [COMF], 2014, art. 272).

no son las responsables directas del manejo de los datos personales ni pueden disponer de ellos libremente.

En este contexto, como última pregunta realizada. La misma versa sobre los mecanismos que existen para que los usuarios financieros puedan reportar vulneraciones a su privacidad. El funcionario de la Superintendencia de Bancos menciono que esta institución tiene mecanismos tanto virtuales como presenciales para los ingresos de quejas, consultas y reclamos. Además, dentro de cada entidad financiera, existe un defensor al cliente, quien es un facilitador y solucionador de conflictos entre las partes y que además, sus servicios no tienen ningún costo para el reclamante. Sin embargo, en el caso específico de una vulneración a la privacidad por el mal uso de datos personales ¿La Superintendencia puede aplicar las sanciones de la Ley de Protección de datos?

3.2 IMPORTANCIA DE UN ORGANISMO DE CONTROL PARA LA PROTECCIÓN DE DATOS PERSONALES

Tanto la supervisión para el cumplimiento de la protección de los datos personales como el control de las actuaciones de las entidades financieras son pilares esenciales para garantizar el derecho a la privacidad y el manejo adecuado de la información de los usuarios. En este contexto, los organismos de control juegan un rol fundamental, no solo para asegurar el cumplimiento de la normativa, sino también para proteger los intereses de los individuos frente a posibles vulneraciones hacia su privacidad.

A nivel internacional, el Consejo de Protección de Datos Europeo ,es un referente clave en la supervisión del tratamiento de datos personales, estableciendo directrices y asegurando la aplicación uniforme del Reglamento General de Protección de Datos en todos los Estados miembros de la Unión Europea. Su función es vital para coordinar las acciones de las autoridades nacionales y garantizar una protección coherente y efectiva de los derechos de los ciudadanos europeos.

Por otro lado, en Ecuador, los organismos encargados de la supervisión y control en este ámbito son la Superintendencia de Bancos y la recientemente creada Superintendencia de Protección de Datos. La primera se centra en el control de las instituciones financieras, garantizando la transparencia y la solvencia del sistema bancario, mientras que la segunda, creada recientemente, tiene como objetivo principal

velar por la correcta gestión y protección de los datos personales en todos los sectores, incluidos los financieros.

3.2.1 LEGISLACIÓN COMPARADA

La protección de datos personales ha cobrado una importancia creciente a nivel internacional, y Europa se ha posicionado como líder en la implementación de marcos regulatorios sólidos. En este contexto, el Consejo Europeo de Protección de Datos (CEPD) y la legislación española en materia de protección de datos destacan por su enfoque integral y avanzado. El CEPD, órgano independiente de la Unión Europea, se encarga de garantizar la aplicación coherente del Reglamento General de Protección de Datos (RGPD) en todos los Estados miembros, promoviendo estándares elevados para la seguridad y el manejo de la información personal.

En España, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) complementa y adapta el RGPD al contexto nacional, ampliando la protección en ámbitos específicos y proporcionando directrices adicionales. Esta legislación establece derechos y obligaciones para los responsables del tratamiento de datos, asegurando que la gestión de la información respete los principios de transparencia, legalidad y confidencialidad. A través de este análisis comparado, se explorarán los principales aspectos de la normativa europea y española, considerando sus contribuciones al desarrollo de políticas de protección de datos.

3.2.2 CONSEJO DE PROTECCIÓN DE DATOS EUROPEO

El Consejo de Protección de Datos Europeo, es un organismo independiente encargado de garantizar la aplicación coherente del Reglamento General de Protección de Datos en toda la Unión Europea. Establecido en el año 2018, reúne a las autoridades de protección de datos de cada Estado miembro y actúa como un mecanismo de supervisión y coordinación entre estos países. Su misión principal es proteger los derechos fundamentales de los individuos en relación con el tratamiento de sus datos personales, promoviendo normas y políticas claras que refuercen la confianza de los ciudadanos en el uso de sus datos.

De esta forma, su principal objetivo es asegurar la implementación constante del derecho fundamental a la protección de datos, reconocido en la Carta de los Derechos

Fundamentales de la Unión Europea. (Comité Europeo de Protección de Datos, 2024). Debido al rápido crecimiento en la transferencia de datos personales, la postura de la Unión Europea en materia de protección de datos debe fortalecerse en el marco de todas sus políticas. Las medidas adoptadas por la Comisión Europea en materia de protección de datos tienen como objetivo establecer un derecho uniforme para todos los estados miembros de la Unión Europea, independientemente del lugar en el que se realice el tratamiento de dichos datos.

Así, mediante la aplicación del Reglamento General de Protección de Datos, se busca dar protección a los datos personales proporcionando.Consediendo a las personas físicas derechos jurídicamente protegidos, establece las responsabilidades de los responsables del tratamiento de datos dentro de las instituciones y organismos de la Unión Europea, y crea una entidad de control autónoma, el Supervisor Europeo de Protección de Datos, encargado de supervisar cómo se gestionan los datos personales dentro de dichas instituciones y organismos (Diario Oficial de la Unión Europea , 2018)

La normativa de la Unión Europea en materia de protección de datos garantiza derechos específicos a las personas y establece un marco de responsabilidad para quienes gestionan los datos dentro de las instituciones y organismos de la Unión. Este marco responde a la necesidad de proteger la privacidad y seguridad de los datos personales, y lo hace imponiendo obligaciones claras y precisas a los responsables del tratamiento de estos datos.

Los responsables del tratamiento dentro de las instituciones y organismos de la Unión deben cumplir con una serie de principios y obligaciones, como la transparencia, la limitación de propósito, y la minimización de datos, que limitan el alcance del tratamiento exclusivamente a lo necesario para cumplir los fines legítimos de la institución. Estos principios aseguran que el tratamiento sea proporcional y adecuado para garantizar los derechos de los individuos.

Además, los responsables tienen el deber de implementar medidas de seguridad técnicas y organizativas apropiadas para proteger los datos personales frente a accesos no autorizados, pérdida o alteración. Estas obligaciones refuerzan la confianza en las instituciones y aseguran que cualquier tratamiento de datos personales esté bajo un sistema de control estricto, minimizando riesgos para la privacidad.

Una vez analizados los objetivos del Reglamento General de Protección de Datos, es necesario que esto se haga efectivo mediante un organismo de control que garantice la protección de datos. En el caso europeo se conformó el Supervisor Europeo de Protección de Datos (SEPD), siendo su principal objetivo velar porque, al manejar datos personales, las instituciones y organismos de la UE respeten el derecho de los ciudadanos a la privacidad. (Supervisor Europeo de Protección de Datos, 2024). La figura del Supervisor Europeo de Protección de Datos actúa como la autoridad de control independiente encargada de supervisar y garantizar que las instituciones y organismos de la Unión cumplan con las obligaciones de tratamiento de datos. Este organismo tiene facultades de auditoría, control y, en su caso, sanción, lo que le permite verificar el cumplimiento de las normativas de protección de datos y asegurar que se respeten los derechos de los titulares de datos

La independencia del SEPD es fundamental para su eficacia, ya que permite una supervisión sin influencias políticas o administrativas, lo cual es esencial para mantener la integridad y la objetividad en la vigilancia. Este modelo de supervisión independiente es un estándar en la protección de datos de la Unión Europea, y representa un compromiso de las instituciones con la transparencia y la rendición de cuentas en el tratamiento de datos personales.

De forma, el modelo europeo enfatiza un equilibrio entre el tratamiento legítimo de datos por parte de las instituciones y la salvaguarda de los derechos individuales, estableciendo para ello un marco robusto de obligaciones y mecanismos de supervisión. La UE demuestra, a través de este sistema, que el respeto a la privacidad y la protección de datos personales son valores fundamentales, y que cualquier uso de datos debe contar con salvaguardas suficientes para asegurar el respeto de estos derechos esenciales. Este modelo puede servir de referencia para otras jurisdicciones en su búsqueda de un marco de protección de datos efectivo y respetuoso de los derechos humanos.

3.2.3 MANEJO DE DATOS CREDITICIOS EN ESPAÑA

El manejo de datos crediticios en España se ha convertido en un aspecto fundamental de la regulación financiera y de la protección de datos personales. En un contexto donde la información crediticia de los individuos se utiliza para evaluar la solvencia y el riesgo en las relaciones financieras, es esencial contar con un marco

normativo que no solo garantice la veracidad y exactitud de estos datos, sino también la protección de los derechos de los titulares.

España, como miembro de la Unión Europea, ha adoptado una serie de normativas alineadas con el Reglamento General de Protección de Datos (RGPD), el cual establece los principios y derechos básicos para la protección de los datos personales. En el ámbito crediticio, esto se complementa con leyes y regulaciones específicas que abordan temas como el tratamiento de la información crediticia, la transparencia en el acceso a estos datos y las obligaciones de las entidades financieras en cuanto a su gestión, teniendo así su propia normativa conocida como Ley Orgánica, de Protección de Datos Personales y garantía de los derechos digitales.

Este acápite explorará los principales aspectos de la normativa española en torno a los datos crediticios, enfocándose en cómo se estructura el sistema de información crediticia y las implicaciones para la privacidad de los usuarios financieros. Además, se analizarán las responsabilidades de las entidades que gestionan estos datos y el papel de las autoridades de control, como la Agencia Española de Protección de Datos (AEPD), en la supervisión y cumplimiento de estas normativas.

Así, se busca entender cómo el sistema español protege los derechos de los titulares de datos frente a posibles abusos y cómo se garantiza un equilibrio entre la necesidad de acceso a la información crediticia y el respeto a la privacidad de los individuos.

Para empezar, se debe establecer que la legislación española mediante su ley orgánica busca adaptar su ordenamiento jurídico al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, también conocido como RGPD. Al adaptarse a este reglamento, la ley no solo asegura que el tratamiento de datos en España cumpla con estándares europeos, sino que también busca completar y aclarar algunos aspectos del reglamento en el contexto español. De esta manera, la Ley Orgánica 3/2018 funciona como una norma complementaria que aborda situaciones específicas del entorno jurídico y social en España, reforzando el derecho fundamental de las personas físicas a la

protección de datos personales, tal como lo consagra el artículo 18.4[23] de la Constitución Española.

Así, se puede subrayar que tanto la legislación ecuatoriana como la española comparten el objetivo de proteger la privacidad y los derechos fundamentales de los ciudadanos. Sin embargo, la Constitución Española destaca un aspecto particular al abordar la influencia de la tecnología, estableciendo que el uso de la tecnología debe estar limitado y regulado por la ley. Esto implica que no se permite el tratamiento indiscriminado de la información personal y que deben existir normas específicas para proteger a los ciudadanos frente a posibles abusos. La intención es asegurar que el desarrollo y uso de la tecnología no vulneren derechos fundamentales. Estos derechos fundamentales que están protegidos en la Constitución refuerzan la importancia del respeto a la privacidad. La referencia a la "intimidad familiar" sugiere que no solo se protege la privacidad individual, sino también el espacio compartido en el ámbito familiar, resguardando las relaciones y la vida personal de intromisiones no autorizadas. La mención del "pleno ejercicio de sus derechos" enfatiza que la protección de la privacidad y el honor es esencial para el ejercicio de otros derechos fundamentales. La privacidad es vista como una condición necesaria para que los ciudadanos puedan disfrutar de sus derechos.

De esta manera, la mencionada Ley Orgánica española establece cinco principios fundamentales en los que debe basarse la protección de datos. Estos principios son similares a los contemplados en la legislación ecuatoriana, esto se debe a que la Ley Orgánica de Protección de Datos Personales de Ecuador es, en esencia, una adaptación de la normativa española, con algunas diferencias. El primer principio se basa en la exactitud de los datos. Que contenido en el artículo 4 de su Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, el primer apartado del artículo reitera la exigencia establecida en el Reglamento (UE) 2016/679 (RGPD), donde establece que los datos personales deben ser exactos y, cuando sea necesario, actualizados. Esto se alinea con la obligación general de los responsables de tratamiento. Además , se garantiza que la información que manejan es correcta y pertinente para los fines para los cuales se recopila. La exactitud es fundamental para proteger los derechos

[23] Artículo 18. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (Cortes Generales, 1978, BOE-A-1978- 31229).

de los individuos, ya que los datos inexactos pueden llevar a decisiones erróneas que afecten negativamente a los individuos.

El segundo apartado detalla que la inexactitud de los datos no será atribuible al responsable del tratamiento si este ha tomado todas las medidas razonables para suprimir o rectificar los datos. Esto introduce una clara distinción en la responsabilidad, enfatizando que el responsable no es automáticamente responsable de la inexactitud de los datos si ha actuado diligentemente. Se plantean cuatro escenarios en los que la responsabilidad puede ser atenuada:

- **Datos obtenidos directamente del afectado**: Si el responsable obtiene datos directamente de la persona interesada, se espera que esta proporcione información precisa. Sin embargo, si hay inexactitudes, el responsable debe actuar rápidamente para corregirlas.

- **Datos obtenidos a través de un intermediario**: Si los datos han sido recopilados por un mediador o intermediario, este último asumirá la responsabilidad en caso de que la información no sea precisa. Esto subraya la importancia de la cadena de responsabilidad en el tratamiento de datos y la necesidad de que los intermediarios también actúen con diligencia.

- **Datos recibidos de otro responsable mediante portabilidad**: En este caso, el artículo señala que si los datos han sido transferidos conforme al derecho de portabilidad, el responsable que recibe los datos no será responsable por la exactitud original de la información. En tendiéndose así que esté se basa en el derecho que tiene la persona afectada a recibir los datos personales que le conciernen, los cuales haya proporcionado a un responsable del tratamiento, en un formato estándar y legible por máquinas, y a transmitirlos a otro responsable sin que este pueda impedirlo.

Es decir, el derecho a la portabilidad de los datos, tal como se describe, establece que los afectados tienen el derecho a recibir sus datos personales en un formato que sea estructurado, de uso común y de lectura mecánica. Este derecho está diseñado para facilitar la transferencia de datos entre diferentes responsables del tratamiento, asegurando que el interesado pueda controlar mejor su información personal y decidir a quién la comparte. Estableciendo así que este derecho aplica solamente en dos principales circunstancias. La primera es cuando el tratamiento se base en la ejecución de un contrato

o bien por el consentimiento y el segundo cuando el tratamiento se efectúe por medios automatizados.

Por ejemplo, en el primer caso se puede dar cuando un cliente tiene un contrato de servicios de telefonía móvil que incluye el almacenamiento de sus registros de llamadas y mensajes. Si el cliente decide cambiar de proveedor de servicios, puede solicitar que sus datos de uso, como el historial de llamadas y mensajes, se transfieran al nuevo proveedor, dado que estos datos son necesarios para la correcta ejecución del nuevo contrato. Aquí, el derecho a la portabilidad se aplica porque el tratamiento de datos está vinculado a la ejecución de un contrato.

El segundo caso basado en el consentimiento se puede ejemplificar en un usuario, el cual se suscribe a un servicio de música en línea, como Spotify. Al registrarse, el usuario da su consentimiento para que la plataforma recopile y procese sus datos personales, como su lista de reproducción y preferencias musicales. Si el usuario decide cambiar a otro servicio, como Apple Music, tiene derecho a solicitar que sus listas de reproducción y datos de escucha sean transferidas a la nueva plataforma, siempre que este tratamiento se base en su consentimiento inicial.

El tercer caso que se basa en el tratamiento por medios automatizados se puede ejemplificar en una aplicación de finanzas personales que recopila automáticamente datos de cuentas bancarias del usuario y las categoriza para ofrecer análisis de gastos. Si el usuario decide cambiar a otra aplicación de finanzas, tiene derecho a solicitar que sus datos financieros, procesados automáticamente por la primera aplicación, se transfieran a la nueva aplicación. La portabilidad en este caso facilita el acceso a información relevante y la continuidad en el uso de servicios digitales, que dependen de un tratamiento automatizado.

- **Datos obtenidos de registros públicos**: Cuando los datos son extraídos de registros públicos, el responsable del tratamiento no es responsable de su exactitud, dado que esta información está oficialmente disponible y se presume que ha sido verificada. Sin embargo, esto no exime a la entidad de la obligación de tratar los datos de manera responsable.

Como segundo principio, la legislación española en el artículo 5 establece el deber de confidencialidad, donde todos los responsables y encargados del tratamiento de

datos, así como cualquier persona que intervenga en el proceso, están sujetos a un deber de confidencialidad. Este deber implica que deben proteger la información personal de los individuos y no divulgarla sin autorización. Esta disposición es coherente con el Reglamento General de Protección de Datos (RGPD), que también subraya la importancia de la confidencialidad en el tratamiento de datos personales. Esto de igual forma se complementa con la legislación ecuatoriana, donde se hace referencia al secreto profesional, pues dentro de la legislación española se establece que la obligación de confidencialidad es complementaria a los deberes de secreto profesional que puedan estar establecidos en otras normativas aplicables. Esto significa que, además de las obligaciones derivadas de la legislación de protección de datos, los profesionales que manejan información sensible como abogados o médicos deben también cumplir con las normas específicas de secreto profesional en sus respectivas áreas. Esta dualidad refuerza la protección de la privacidad y la confidencialidad de los datos personales en múltiples niveles.

Además, la legislación extranjera menciona que las obligaciones de confidencialidad se mantienen incluso después de que haya finalizado la relación bien sea está laboral o contractual entre el titular y el responsable de los datos. Esto es crucial para garantizar que la información sensible siga protegida, incluso una vez que la persona que tenía acceso a ella ya no esté en el cargo. Esta disposición es fundamental para la confianza de los individuos en el manejo de sus datos, ya que asegura que su información no será divulgada o utilizada inapropiadamente.

El deber de confidencialidad es un pilar esencial en la protección de datos personales, que busca garantizar la confianza de los usuarios en el uso de sus datos. La inclusión de normas complementarias, como el secreto profesional, y la duración indefinida , de estas obligaciones fortalecen la seguridad jurídica en la gestión de datos. A través de estas disposiciones, se busca prevenir filtraciones de datos y asegurar que la información personal sea manejada con el máximo respeto y cuidado.

El tercer principio versa en el tratamiento basado en el consentimiento del afectado. De esta forma la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales establece que el consentimiento debe ser una manifestación de voluntad libre donde el afectado debe tener la capacidad de decidir sin coerción o presión, haciendo referencia a que el consentimiento debe tener un propósito concreto y no ser

general o vago. Se considera informado cuando el afectado debe recibir información suficiente sobre qué implica el tratamiento de sus datos y para qué se utilizarán, e, inequívoca cuando se establece que el consentimiento debe ser claro, ya sea a través de una declaración o una acción afirmativa

Es importante además establecer que, cuando se requiera el consentimiento para múltiples finalidades, debe ser específico e inequívoco para cada una de ellas. Esto significa que los responsables del tratamiento no pueden asumir que el consentimiento para una finalidad se extiende automáticamente a otras; deben asegurarse de que el afectado entienda y acepte explícitamente cada propósito. Esto promueve una mayor transparencia y autonomía del individuo sobre cómo se utilizan sus datos. Quedando totalmente prohibido que se condicione la ejecución de un contrato para conseguir el consentimiento del afectado para el tratamiento de datos con finalidades que no estén directamente relacionadas con el mantenimiento, desarrollo o control de la relación contractual. Esto es crucial para proteger a los consumidores y evitar abusos, asegurando que los individuos no se vean forzados a aceptar el tratamiento de sus datos personales como una condición para acceder a un servicio o producto.

Ahora bien, para analizar el cuarto principio es necesario mencionar que dentro de este existe una diferencia con la legislación ecuatoriana, esto debido a que mientras esta considera que el tratamiento de datos de menores de edad es una categoría especial; la legislación española lo establece como un principio para el manejo de protección de datos. Mismo que establece dos formas para el manejo de datos personales de los menores de edad. El primero hace referencia a tratamiento de datos personales de un menor, solo puede basarse en su propio consentimiento una vez que ha alcanzado los catorce años. Esto significa que, a partir de esta edad, los menores tienen la capacidad legal de consentir el tratamiento de sus datos, siempre que se trate de situaciones en las que no se requiera la intervención de los titulares de la patria potestad o tutela. Este enfoque busca fomentar la autonomía de los jóvenes en el manejo de su información personal, alineándose con el principio de autonomía progresiva, que reconoce que los menores, a medida que crecen, deben participar en decisiones que les afectan.

Y el segundo caso versa en el tratamiento de datos de los menores de catorce años. El tratamiento de datos personales solo será legal si se cuenta con el consentimiento de los titulares de la patria potestad o tutela. Esta disposición es crucial para proteger a los

menores que, debido a su edad, pueden no tener la madurez suficiente para comprender completamente las implicaciones del tratamiento de sus datos. Al requerir el consentimiento de los padres o tutores, se busca salvaguardar los intereses de los menores y garantizar que su información personal sea tratada de manera responsable y segura.

Como quinto principio está el tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos. Donde se establece que el tratamiento de datos personales puede fundamentarse en el cumplimiento de una obligación legal que esté exigida al responsable del tratamiento. El tratamiento de datos personales puede considerarse legal si está fundamentado en una misión realizada en interés público o en el ejercicio de poderes públicos.

- **Interés público**: Esta cláusula permite que los datos sean tratados para fines que beneficien a la sociedad, como la protección de la salud pública, la educación, o la seguridad.

- **Poderes públicos**: El tratamiento debe estar claramente definido por la legislación que otorga competencias específicas a los organismos públicos.

El principio mencionado se aplica de manera similar a la legislación ecuatoriana, en cuanto al tratamiento de datos que sea necesario para el interés público. En ambas normativas, se reconoce la importancia de llevar a cabo el tratamiento de datos personales cuando este responde a necesidades de carácter público, garantizando así que las acciones en este ámbito estén alineadas con el bienestar general de la sociedad.

Esta convergencia en la regulación resalta un enfoque común hacia la protección de los derechos de los individuos, a la vez que se permite el uso responsable de la información personal en beneficio de la comunidad.

3.2.4 SISTEMAS DE INFORMACIÓN CREDITICIA

Los sistemas de información crediticia juegan un papel fundamental en el ámbito financiero, ya que permiten la evaluación del riesgo crediticio de los solicitantes de créditos y préstamos. En España, la regulación de estos sistemas está principalmente enmarcada en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos

Personales y Garantía de los Derechos Digitales, que establece un conjunto de principios y derechos relacionados con el tratamiento de datos personales, incluidos aquellos referidos a la información crediticia. La legislación española reconoce la importancia de proteger la información personal de los individuos, al tiempo que facilita la actividad de las entidades financieras y los servicios de información crediticia. En este contexto, se establece que los datos sobre la solvencia de un consumidor solo pueden ser tratados cuando existan bases legales adecuadas, como el cumplimiento de una obligación legal o el interés legítimo del responsable del tratamiento, siempre que se respeten los derechos de los interesados.

Además, la Ley de Protección de Datos y el Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos o RGPD) garantizan que la información proporcionada por los consumidores sea precisa y actualizada, y otorgan a los individuos derechos específicos, como el derecho a acceder, rectificar y suprimir sus datos. Este marco legal busca equilibrar la necesidad de las entidades financieras de evaluar la capacidad de pago de los clientes y la protección de la privacidad y los derechos de estos últimos.

Para entender a que hace referencia el sistema de información crediticia se debe partir estableciendo que estos son "Los registros de morosos, también conocidos como ficheros de solvencia patrimonial o sistemas de información crediticia, son registros que recogen datos de impago, ya sea de personas físicas o jurídicas, sobre deudas dinerarias, crediticias o financieras" (Comunidad de Madrid, 2024). Es decir, son ficheros en los que se recogen deudas contraídas por las personas consumidoras como resultado de alguna operación comercial.

En este contexto, el manejo de datos crediticios dentro de la legislación española está dispuesto en el artículo 20 de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. Así, para empezar con este análisis se debe partir de la Presunción de Licitud, este artículo establece que, salvo prueba en contrario, el tratamiento de datos sobre incumplimientos es presumido lícito si se cumplen los siguientes requisitos:

- **Procedencia de los Datos**: Este requisito establece que los datos deben ser proporcionados por el acreedor o por alguien que actúe en su nombre. Esto

garantiza que la información utilizada en los sistemas de información crediticia sea legítima y verificada, lo que reduce la posibilidad de errores o abusos en el tratamiento de datos, otorgando así una responsabilidad a las entidades financieras al momento de utilizar estos ficheros debido a que "la inclusión indebida en ficheros de morosidad produce unos efectos especialmente negativos para los ciudadanos afectados en relación con el acceso a todo tipo de servicios, por los que las empresas han de extremar su diligencia antes de comunicar información inexacta a los mismos" (Ac Abogados, 2024).

En este contexto, la inclusión errónea en ficheros de morosidad puede tener consecuencias especialmente perjudiciales para los ciudadanos, ya que afecta su acceso a una variedad de servicios. Esta situación puede derivar en la negación de créditos, la imposibilidad de suscribir contratos y restricciones en la obtención de productos y servicios básicos, lo que, a su vez, agrava su situación económica y financiera.

Por lo tanto, es fundamental que las empresas actúen con la máxima diligencia al proporcionar información sobre deudas. Esto incluye verificar la exactitud de los datos antes de reportarlos a los sistemas de información crediticia, para así evitar que los consumidores sean perjudicados por información incorrecta. La responsabilidad de las entidades que manejan datos crediticios es crítica, ya que su actuación puede influir significativamente en la vida y las oportunidades de los individuos afectados.

- **Naturaleza de las Deudas:** Se requiere que las deudas sean ciertas, vencidas y exigibles, lo que significa que solo se puede incluir información sobre obligaciones que el deudor realmente ha dejado de pagar y que no han sido disputadas mediante reclamaciones. Esto protege a los deudores de ser penalizados por deudas que pueden no ser válidas o que están en disputa, " Es decir, es necesario que se trate de deudas realmente existentes, sin términos o condiciones pendientes de finalización o cumplimiento, de cuantía determinada y cuyo cumplimiento pueda exigirse por vía judicial" (Ac Abogados, 2024).

  Por lo tanto, La inclusión de datos en registros de morosidad está restringida exclusivamente a deudas de carácter dinerario, lo que implica que solo se pueden

registrar aquellas obligaciones que impliquen un pago de dinero. Esto se traduce en que cualquier relación contractual que no esté relacionada con el incumplimiento de obligaciones monetarias queda excluida de la posibilidad de ser reportada en estos ficheros.

Por ejemplo, si una obligación se refiere a una prestación de servicios personales o a un contrato que no implique un pago específico, no podrá dar lugar a la inclusión de datos en sistemas de información crediticia. Asimismo, cualquier información que no esté vinculada directamente a deudas dinerarias, como datos sobre solvencia patrimonial o crédito que no se refieran a obligaciones específicas, también debe ser excluida de estos registros.

- **Información al Afectado:** Se debe notificar al afectado, ya sea en el contrato o en el aviso previo de pago, sobre la posibilidad de que sus datos sean incluidos en un determinado SIC (Ac Abogados, 2024). En este sentido, el acreedor debe informar al deudor sobre la posibilidad de que su deuda sea incluida en el sistema de información crediticia, ya sea en el contrato o al momento de requerir el pago. Además, se establece una obligación de notificación posterior sobre la inclusión de datos, permitiendo al afectado ejercer sus derechos bajo el RGPD en un plazo de treinta días. Este requisito de transparencia es fundamental para garantizar que los deudores estén informados y puedan actuar.

- **Duración de la Conservación de Datos:** los datos solo pueden ser mantenidos en el sistema mientras persista el incumplimiento, y se establece un límite máximo de cinco años desde la fecha de vencimiento de la obligación. Esta limitación temporal es crucial para evitar que los deudores sean penalizados indefinidamente por deudas pasadas y para asegurar que la información crediticia refleje su situación actual.

- **Consultas de Datos:** La consulta de los datos del deudor solo puede realizarse por aquellos que mantengan una relación contractual con el afectado que implique algún tipo de pago. Esto limita el acceso a la información sensible y protege la privacidad del deudor, asegurando que solo aquellos con un interés legítimo puedan acceder a sus datos.

- **Resultado de Consultas y Negación de Contratos:** Si se deniega la solicitud de un contrato debido a la consulta en el sistema, se requiere que la entidad que

realizó la consulta informe al afectado sobre el resultado. Este requisito de notificación es fundamental para la transparencia y la equidad en el proceso crediticio, permitiendo al deudor comprender porque no se le ha otorgado el crédito.

Además, dentro del manejo de datos crediticios en la legislación española se establece que tanto las entidades que gestionan los sistemas de información crediticia como los acreedores son considerados corresponsables en el tratamiento de los datos relacionados con sus deudores. Esto implica que ambas partes tienen responsabilidades compartidas en cuanto a la correcta inclusión y manejo de la información crediticia. Según el Reglamento (UE) 2016/679, específicamente en su artículo 26[24], esto significa que deben colaborar para asegurarse de que se cumplan todas las exigencias legales antes de que una deuda sea reportada.

Y para finalizar, la presunción de licitud en la inclusión de datos no se aplica en casos donde la información crediticia se relacione con datos adicionales obtenidos de otras fuentes, especialmente si se utilizan para el perfilado del deudor. Esto resalta la importancia de limitar el uso de información a lo estrictamente necesario y relacionado con el incumplimiento de obligaciones dinerarias. La práctica de asociar datos adicionales para realizar un perfilamiento, especialmente a través de técnicas de calificación crediticia, no está permitida en este contexto, lo que protege aún más la privacidad de los consumidores y evita la discriminación o el uso indebido de su información.

Por ejemplo, si un acreedor intenta incluir datos de un sistema de calificación crediticia que considera el historial de compra del deudor su actividad en redes sociales, esto violaría las normativas que protegen la privacidad y limitan el uso de datos aquellos estrictamente necesarios para determinar la solvencia. Esto garantiza que los consumidores no sean objeto de decisiones discriminatorias basadas en información que no está relacionada directamente con su capacidad de pago de obligaciones.

3.2.5 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La Agencia Española de Protección de Datos (AEPD) es la autoridad competente en España para velar por el cumplimiento de la normativa de protección de datos,

garantizando el derecho fundamental a la privacidad y a la protección de datos personales de los ciudadanos. La AEPD desempeña un papel crucial en la supervisión y promoción de la correcta aplicación del Reglamento General de Protección de Datos (RGPD) y de la legislación nacional, ofreciendo orientación y recursos tanto a individuos como a organizaciones sobre sus derechos y obligaciones en materia de protección de datos.

Ahora bien, el decreto real número 389/2021 dispone que la función principal es velar por el cumplimiento de las leyes sobre protección de datos personales, con el propósito de salvaguardar los derechos y libertades de las personas en lo que concierne al procesamiento de sus datos (Real Decreto 389/2021, 2021, art. 5), pero además, cada organismo de control debe cumplir con lo establecido en el reglamento (UE) 2016/679 del Parlamento Europeo. Además de sus funciones de control y supervisión, la AEPD actúa como un ente educativo, promoviendo la conciencia sobre la importancia de la privacidad y la protección de la información personal. También colabora con otras agencias de protección de datos a nivel internacional para abordar desafíos globales en la gestión de datos, adaptándose a los constantes cambios tecnológicos y a la evolución de la economía digital.

Así, contar con un organismo de control como la Agencia Española de Protección de Datos es fundamental para asegurar el cumplimiento de la normativa de protección de datos y defender los derechos de los ciudadanos, en un mundo cada vez más digitalizado. La AEPD no solo supervisa y sanciona posibles incumplimientos, sino que también educa y fomenta la conciencia sobre la privacidad y la gestión responsable de la información personal. En una sociedad donde los datos personales tienen un valor inmenso y están expuestos a riesgos, la AEPD desempeña un rol indispensable, ofreciendo orientación y promoviendo la colaboración internacional para enfrentar los desafíos en la protección de datos. Su función de vigilancia y adaptación a los cambios tecnológicos y económicos es esencial para que el derecho a la privacidad se mantenga protegido en el entorno digital actual.

3.2.6 SUPERINTENDENCIA DE PROTECCIÓN DE DATOS EN EL ECUADOR

En el contexto ecuatoriano, recientemente se creó la Superintendencia de protección de datos, teniendo, así como su principal función vigilar y regular el manejo de datos personales, teniendo además, la autoridad para imponer sanciones de acuerdo

con la Ley Orgánica de Protección de Datos Personales (Consejo de Participación Ciudadana y Control Social, S.F). De esta forma, la creación de la Superintendencia de Protección de Datos en Ecuador es un paso fundamental para garantizar la efectiva aplicación de la Ley Orgánica de Protección de Datos Personales, promulgada en 2021. Esta institución tiene como responsabilidad supervisar y controlar el tratamiento de los datos personales, así como la autoridad de imponer sanciones en casos de incumplimiento. En un contexto en el que los datos personales se han convertido en un activo económico, la venta y manipulación de esta información es una práctica común, y muchas veces ocurre sin el consentimiento de los titulares de los datos. Esto convierte en imprescindible la existencia de un órgano que vele por los derechos de privacidad y protección de datos de los ciudadanos ecuatorianos.

Sin embargo, ha resultado contraproducente que esta ley entrara en vigor sin contar previamente con una autoridad capaz de hacerla cumplir. Esta omisión generó una brecha significativa en la protección de los derechos de los ciudadanos, ya que sin una entidad reguladora, las normas pierden su efectividad y se dificultan los esfuerzos para hacer cumplir los principios de privacidad establecidos en la legislación. La creación tardía de esta superintendencia ha dejado a Ecuador en una situación vulnerable, permitiendo que tanto entidades públicas como privadas continúen con prácticas de tratamiento de datos sin supervisión, lo cual puede derivar en la explotación indebida de datos personales. La Superintendencia de Protección de Datos es crucial, pues permitirá que el derecho a la protección de datos se respete y se consolide, creando un entorno en el que las instituciones tengan que cumplir con los estándares de seguridad y privacidad de datos personales.

3.3 CONCLUSIONES

En conclusión, tras analizar el contexto de la protección de datos en el Ecuador, se puede afirmar que las entidades financieras no son directamente responsables del uso indebido de los datos personales en la gestión de cobros. Estas instituciones generalmente cumplen con sus obligaciones informativas, especificando en sus políticas de privacidad que el uso de datos puede incluir la comercialización de información en el marco de servicios financieros. No obstante, el problema surge con las compañías auxiliares de cobranza, que son quienes realizan llamadas para gestionar obligaciones. En muchos casos, estas empresas contactan no solo a los deudores, sino también a terceros sin

autorización, lo cual representa una clara vulneración del derecho a la privacidad, tanto para los deudores como para las personas no vinculadas que no dieron su consentimiento para el tratamiento de sus datos. Esta práctica afecta el derecho a la privacidad y el uso informado de los datos personales, y es un problema agravado por la venta constante de bases de datos en Ecuador.

La protección de datos personales en Ecuador enfrenta una serie de desafíos significativos, especialmente en el sector financiero, donde la privacidad de los usuarios y su derecho a controlar su información personal se ven amenazados por la constante circulación y comercialización de sus datos. A lo largo de este estudio, se ha analizado cómo el tratamiento de datos personales por parte de entidades financieras y empresas auxiliares de cobranza afecta la privacidad de los ciudadanos, y se han evaluado los mecanismos legales y de supervisión existentes para salvaguardar estos derechos.

En primer lugar, es importante destacar que las entidades financieras, en general, han implementado políticas de privacidad que informan a los usuarios sobre el tratamiento de sus datos. Este cumplimiento normativo, aunque necesario, no garantiza la protección completa de la privacidad de los clientes, dado que las empresas de cobranza, contratadas como auxiliares de estas entidades, suelen recurrir a prácticas invasivas que exceden el límite del consentimiento otorgado. Esto pone de manifiesto una vulnerabilidad en el sistema, donde, a pesar de la transparencia en las políticas de privacidad, no existe un control eficaz sobre el tratamiento de los datos personales.

La normativa ecuatoriana, en su intento por adaptarse a estándares internacionales, ha introducido la Ley Orgánica de Protección de Datos Personales (LOPDP), la cual establece principios claros y directrices sobre el tratamiento adecuado de la información personal. Sin embargo, la ausencia de un organismo sancionador específico ha retrasado su aplicación efectiva. Si bien la Superintendencia de Bancos es el órgano de supervisión en el ámbito financiero, pero carece de la facultad para sancionar vulneraciones específicas en materia de datos personales, especialmente en casos de prácticas abusivas por parte de terceros.

Esta situación ha derivado en un vacío de control que impacta directamente en los derechos de los ciudadanos. En un contexto donde los datos se comercializan con frecuencia y sin control aparente, los usuarios ven vulnerados sus derechos sin contar con una instancia efectiva a la cual recurrir. Es en este punto donde la creación de la

Superintendencia de Protección de Datos cobra relevancia. La existencia de este organismo especializado permite una supervisión más cercana y estricta del tratamiento de datos en el país, estableciendo la posibilidad de sancionar directamente a aquellos que infringen la normativa.

La función de la Superintendencia de Protección de Datos no solo es crucial en términos de control y sanción, sino que también es fundamental para fomentar una cultura de privacidad en Ecuador. Mediante campañas de concientización y el desarrollo de guías prácticas para las entidades, este organismo puede promover una comprensión más amplia sobre el derecho a la privacidad, educando a las empresas como a los ciudadanos sobre las prácticas en el manejo de información personal.

La importancia de este órgano regulador también radica en su capacidad para imponer una estructura de cumplimiento clara y eficiente, en la cual tanto entidades financieras como empresas de cobranza deban operar bajo normas que garanticen el respeto por la privacidad del individuo. Este tipo de supervisión reduce el riesgo de prácticas abusivas, asegurando que la información personal de los ciudadanos no sea utilizada de manera indebida o con fines de presión indebida para el cobro de deudas.

Asimismo, es fundamental entender que la implementación de sanciones adecuadas, tanto a nivel económico como administrativo, se convierte en un disuasivo contra la comercialización ilícita de datos. La posibilidad de sancionar a los actores que infringen la normativa establece un precedente que refuerza el compromiso del país con la protección de datos personales y fomenta una mayor confianza en las instituciones.

La situación actual del sector financiero en Ecuador muestra que, aunque se han dado pasos importantes, aún existen deficiencias en la protección efectiva de datos personales. La entrada en vigor de la Superintendencia de Protección de Datos representa un avance significativo, pero su éxito dependerá de la capacidad del organismo para actuar con autonomía y rigor, asegurando que todos los involucrados cumplan con los estándares establecidos en la LOPDP.

Por otro lado, es importante subrayar que la responsabilidad de proteger los datos personales no recae únicamente en el sector financiero o en las entidades de cobranza, sino que requiere un compromiso conjunto de todas las instituciones involucradas y de la sociedad en su conjunto, con una colaboración interinstitucional, resulta esencial para construir un sistema de protección de datos que sea inclusivo y efectivo.

El futuro de la protección de datos en Ecuador dependerá de la efectividad con la que esta Superintendencia ejecute sus funciones, y de la capacidad de las instituciones

para adaptarse a un marco regulatorio que proteja no solo la privacidad de los deudores, sino también de los terceros que se ven afectados indirectamente por las prácticas de cobro indebidas. Con este nuevo enfoque, se espera construir un entorno en el que la confidencialidad de la información personal sea respetada y en el que los derechos de los ciudadanos estén verdaderamente protegidos frente a un uso indebido de sus datos.

Porque a pesar de que rastrear el origen exacto de la cadena de comercialización de datos personales puede resultar imposible, es viable sancionar a quienes, en última instancia, hacen un uso indebido de esta información. En el contexto ecuatoriano, donde la venta de datos personales es una práctica extendida, esta situación no exime a las entidades de su deber de proteger el derecho fundamental a la privacidad. Este derecho debe ser respetado y garantizado para todos los ciudadanos del Ecuador, y es responsabilidad de las autoridades competentes y de las entidades involucradas adoptar las medidas de control necesarias para asegurar su cumplimiento efectivo.

REFERENCIAS

AC Abogados. (s.f.). *Requisitos normativos y jurisprudenciales para la inclusión de datos personales en los ficheros de morosos (sistemas de información crediticia)*. AC Abogados. Recuperado el 5 de noviembre de 2024, de https://www.ac-abogados.es/requisitos-normativos-y-jurisprudenciales-para-la-inclusion-de-datos-personales-en-los-ficheros-de-morosos-sistemas-de-informacion-crediticia/

Agencia Española de Protección de Datos. (s.f.). *Resumen de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales*. Recuperado en noviembre de 2024, de https://www.aepd.es

Agencia Española de Protección de Datos. (2024). *¿Qué es el derecho a la portabilidad de los datos?* https://www.aepd.es

Agencia Española de Protección de Datos. (2021). *Real decreto 389/2021, de 1 de junio, por el que se aprueba el estatuto de la Agencia Española de Protección de Datos*. Boletín Oficial del Estado, n.º 130, pp. 67413–67440. https://www.boe.es/boe/dias/2021/06/01/pdfs/BOE-A-2021-8934.pdf

Aguilar, A., Benítez, E., Scotti, L., & Sorokin. (2022). *La privacidad como derecho humano*. Dirección de Publicaciones de la UCSG. https://editorial.ucsg.edu.ec/archivos/la_privacidad_como_derecho_humano.pdf

Aponte Núñez, E. J. (2007). *La importancia de la protección de datos de carácter personal en las relaciones comerciales: Aproximación al derecho venezolano*. *Revista de Derecho Privado*, 12-13, 109–124.

Azaustre Fernández, M. J. (2008). *El secreto bancario* (Ed.). J.M. Bosch Editor. https://elibro.net/es/lc/uazuay/titulos/36656

Botelho, J. (2012). *Jusformularios: Bancário* (Ed.). La Ley Soluciones Legales S.A. https://elibro.net/es/lc/uazuay/titulos/76127

Buró de Crédito vs. Central de Riesgos. (2024). *Equifax*. https://www.equifax.com.ec/miscreditos/blog/central-de-riesgos

Cadena, A. (2009). *El sigilo, reserva bancaria y el hábeas data en el Ecuador*, [Trabajo de titulación previo a la obtención del título de abogado de los tribunales]. Repositorio Institucional de la Universidad de las Américas. https://dspace.udla.edu.ec/bitstream/33000/527/1/UDLA-EC-TAB-2009-20.pdf

Superintendencia de Bancos. (2024). *Codificación Superintendencia de Bancos, Libro Primero, Tomo IV, reformada, 15 de agosto de 2024* (Ecuador).

Superintendencia de Bancos. (2024). *Codificación Superintendencia de Bancos, Libro Primero, Tomo I, reformada, 16 de febrero de 2024* (Ecuador).

Comunidad de Madrid. (2024). *Saber si estamos en el registro de morosos y cómo salir*. https://www.comunidad.madrid/servicios/consumo/saber-si-estamos-registro-morosos-salir

Consejo de Participación Ciudadana y Control Social. (s.f.). *Nueva Superintendencia de Protección de Datos en Ecuador*. Fundación de Transparencia y Control Social. Recuperado el [2024], de https://ftcs.gob.ec/nueva-superintendencia/#:~:text=La%20Superintendencia%20se%20encarga%20de,de%20Transparencia%20y%20Control%20Social.

Constitución de la República del Ecuador[CRE]. (2024). *30 de mayo de 2024.* (Ecuador).

Corte Constitucional de la República de Colombia. (2010). *Sentencia C-640/10, M.P. María Victoria Calle Correa; 18 de agosto de 2010*.

Corte Constitucional de la República de Colombia. (2014). *Sentencia C-881/14, M.P. María Victoria Calle Correa; 19 de noviembre de 2014*.

Corte Constitucional de la República de Colombia. (2017). *Sentencia T-547/17, M.P. Gloria Stella Ortiz Delgado; 2017*.

Corte Constitucional de la República del Ecuador. (2021). *Caso No. 2064-14-EP, J.P. Carmen Corral Ponce; 27 de enero de 2021*.

Cortes Generales. (1978). *Constitución española*. Boletín Oficial del Estado, núm. 311, 29 de diciembre de 1978. https://www.boe.es/buscar/doc.php?id=BOE-A-1978-31229

Código Orgánico Integral Penal [COIP]. (2024). *29 de julio de 2024* (Ecuador).

Código Orgánico Monetario y Financiero [COMF]. (2024). *Libro I*. 29 de julio de 2024 (Ecuador).

Comité Europeo de Protección de Datos. (s.f.). *European Data Protection Board*. https://www.edpb.europa.eu/edpb_en

De Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. (s.f.). *Revista de Derecho*, 27, 44–65. https://repositorio.uasb.edu.ec/bitstream/10644/5945/1/05-TC-

Naciones Unidas. (1948). *Declaración Universal de los Derechos Humanos*. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Enríquez, L. (2017). *Paradigmas de la protección de datos personales en Ecuador: Análisis del proyecto*.

European Parliament & Council of the European Union. (2023). *Reglamento (UE) 2023/1525 del Parlamento Europeo y del Consejo, de 20 de julio de 2023, relativo al apoyo a la producción de municiones*. EUR-Lex. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023R1525

European Commission. (n.d.). *Aviso de privacidad sobre el Fondo de Asilo, Migración e Integración (AMIF)*. https://commission.europa.eu/document/download/2230f5f6-9b83-45f3-b591-3b9258559a34_es?filename=lef_baf_privacy_notice-es.pdf

Falconi, M. (2022). Cláusulas abusivas y derechos de los consumidores en Ecuador. *Chakiñan*, 18, 192–202. http://scielo.senescyt.gob.ec/pdf/rchakin/n18/2550-6722-rchakin-18-00191.pdf

Flores Dapkevicius, R. (2009). *Manual de derecho público. Vol. I. Derecho constitucional*. Euros Editores S.R.L.

Gacitúa, A. (2014). *El derecho fundamental a la protección de datos personales en el ámbito de la prevención y represión penal europea (en busca del equilibrio entre la libertad y la seguridad)* [Tesis doctoral]. Universidad Autónoma de Barcelona. https://www.tdx.cat/handle/10803/284352#page=1

Kress, A. (2017). *La Unión Europea como modelo de protección de datos en eHealth, su influencia y barreras a la convergencia* [Tesis doctoral, Universitat Politècnica de Catalunya]. https://www.tesisenred.net/handle/10803/406042#page=1

Ley Orgánica de Protección de Datos Personales [LOPDP]. (2024). *No reformada, 26 de mayo de 2024* (Ecuador).

Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. (2018). *Boletín Oficial del Estado*, núm. 294, de 6 de diciembre de 2018. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Lídice, R. (2018). *El contrato de adhesión como instrumento de regulación en las relaciones de consumo y empresariales* (1. ed.). Ediciones Olejnik. https://elibro.net/es/lc/uazuay/titulos/235257

Maza, K. (2022). *La protección de datos en el Ecuador: Un análisis en el derecho comparado* [Trabajo de titulación previo a la obtención del título de abogado de los tribunales]. Repositorio Institucional Uniandes. https://dspace.uniandes.edu.ec/bitstream/123456789/14552/1/USD-DER-EAC-028-2022.PDF

Meins Olivares, E. (2000). Derecho a la intimidad y a la honra en Chile. *Ius et Praxis*, 6(1), 303–319.

Ministerio de Salud Pública del Ecuador. (2021). *Reglamento de información confidencial en el Sistema Nacional de Salud, reformado, 29 de enero de 2021*.

Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador. (2023). *Reglamento de la Ley Orgánica de Protección de Datos Personales, no reformada, 13 de noviembre de 2023*.

Muñoz, C. (2018). *Los contratos de adhesión y el principio de autonomía de la voluntad de las partes en la sociedad ecuatoriana* [Trabajo de titulación previo a la obtención del

título de abogado de los tribunales]. Repositorio Institucional de la Universidad del Azuay. https://dspace.uazuay.edu.ec/bitstream/datos/8312/1/14035.PDF

Normas de control para las entidades de los sectores financieros público y privado. 13 de abril de 2016, (Ecuador).

Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679, de 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*. Diario Oficial de la Unión Europea, L 119, 1–88. Recuperado de https://www.boe.es/doue/2016/119/L00001-00088.pdf

Pfeiffer, M. L. (2008). Derecho a la privacidad. Protección de los datos sensibles. *Revista Colombiana de Bioética*, 3(1), 11–36. https://www.redalyc.org/articulo.oa?id=189217248002

Organización de los Estados Americanos. (2022). *Principios actualizados sobre la privacidad y la protección de datos personales.* https://www.oas.org/es/sla/cji/docs/publicacion_proteccion_datos_personales_principios_actualizados_2021.pdf

Ramírez, M. (2011). *El derecho a la intimidad: Análisis en la normativa ecuatoriana* [El derecho a la intimidad. Análisis en la normativa ecuatoriana]. Repositorio Institucional de la Universidad del Azuay. https://dspace.uazuay.edu.ec/bitstream/datos/5520/1/08518.PDF

Salgado, H. (2008). El derecho a la protección de la vida privada y el derecho a la libertad de información en la doctrina y en la jurisprudencia ecuatoriana. *Estudios Constitucionales*, 1, 69-83. Recuperado de http://bivicce.corteconstitucional.gob.ec/bases/biblo/texto/revista_cecoch/revista-ano6-1-3.pdf

Sanz, F. (2018). Delimitación de las esferas de la vida privada, privacidad e intimidad, frente al ámbito de lo público. *Transparencia y Sociedad*, 6, 127-149. Recuperado de https://www.consejotransparencia.cl/wp-content/uploads/2019/03/TS-N6-ARTICULO5.pdf

Superintendencia de Bancos. (2024). *Bancos*. Superintendencia de Bancos del Ecuador. https://www.superbancos.gob.ec/bancos/

Supervisor Europeo de Protección de Datos. (s.f.). *Supervisor Europeo de Protección de Datos (EDPS)*. Unión Europea. Recuperado el [fecha de consulta] de https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-supervisor-edps_es

Sánchez, M. (2015). *Implicaciones institucionales de la ley de protección de datos* [Tesis doctoral, Universidad de Málaga].

Tigrero, F. (2021). *Análisis de los derechos a la intimidad personal y familiar en relación al cumplimiento de la finalidad del Código Orgánico Integral Penal en el*

Ecuador y en el Código Penal de España [Trabajo de titulación previo a la obtención del título de abogado de los tribunales]. Repositorio Institucional de la Universidad Católica de Cuenca. https://dspace.ucacue.edu.ec/handle/ucacue/9986

Torre, I. S.-T. (2015). Derecho a la intimidad personal en el ámbito laboral. *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, (13), 335-362. https://doi.org/10.18172/redur.4185

Unión Europea. (2018). *Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se deroga el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE*. Diario Oficial de la Unión Europea, L 295, 39-84. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1725

Villanueva, J., & Arias, L. (2010). El secreto bancario. Aspectos históricos y problemática actual. *Diálogos: Revista Electrónica de Historia*, *11*(1), 67-88. https://www.scielo.sa.cr/pdf/dreh/v11n2/a04v11n2.pdf

Vera, M., & Vivero, M. (2019). ¿Vida privada o muerte a la privacidad? *USFQ Law Review*, *6*(1), 233-254.

https://revistas.usfq.edu.ec/index.php/lawreview/article/view/1397/1623

Zavala, J. (2019). Derecho constitucional, neoconstitucionalismo y argumentación jurídica (pp. 279-307). Murillo Editores.

ANEXOS

ENTREVISTAS USUARIOS FINANCIEROS

1. INFORMANTE UNO

1 ¿Qué entiendes por protección de datos personales en el contexto financiero?

La protección de datos personales en contexto financiero se entiende que; una entidad se responsabiliza en resguardar y proteger la administración económica personal, ya sean en cuantas bancarias o tarjetas de crédito, a pesar de esto las entidades bancarias conocen nuestro manejo financiero y nos invitan a adquirir préstamos.

Considerando a terceros como empresa privada o instituciones financieras, sí, ya que cualquier tipo de banco conoce nuestros movimientos bancarios, por lo tanto, nos invitan a que aceptemos ofertas o prestamos, todo esto en base al conocimiento del dinero que recibimos mensualmente y además de como pagamos deudas bancarias o de otras instituciones.

2. ¿Alguna vez has sentido que tu información personal ha sido utilizada sin tu consentimiento por una entidad financiera?

Sí, ya que entidades financieras como bancos o empresas privadas conocen nuestro manejo de cuentas y están constantemente insistiendo en que aceptemos prestamos o que nos endeudemos en promociones u ofertas que ellos patrocinan.

3. ¿Consideras que las entidades financieras te brindan información clara sobre tus derechos en cuanto a la protección de tus datos?

No, personalmente creo que los bancos o cooperativas son un sitio seguro donde guardar el dinero, pero no se conoce los derechos que contamos como usuarios.

4. ¿Crees que las políticas de privacidad de las entidades financieras son claras y accesibles?

No, únicamente creo que las utilizamos para guardar dinero o un sitio donde recibimos el salario de nuestro trabajo, pero jamás se nos explica las políticas de privacidad.

5. ¿Al momento del cobro de deudas, ¿Has sentido que tus datos con revelados? ¿ Cómo afecta esto a tu privacidad?

Sí, definitivamente he sentido que mis datos han sido revelados durante el proceso de cobro de deudas. En varias ocasiones, los cobradores han llamado a mis contactos personales para comunicar mi situación financiera, algo que considero una violación a mi privacidad. Me ha generado mucha incomodidad, ya que siento que la información sobre mi situación económica es algo privado y no debería ser compartida con terceros sin mi consentimiento

2. INFORMANTE DOS

1. ¿Qué entiendes por protección de datos personales en el contexto financiero?

Se refiere al resguardo de la información personal sensible que manejan las entidades financieras. Los datos personales pueden incluir información como ingresos o deudas, como también nombre, número de identificación, y otros.

2. ¿Alguna vez has sentido que tu información personal ha sido utilizada sin tu consentimiento por una entidad financiera?

Sí, en este país siempre. No solo se siente, es de conocimiento público que las bases de datos son comercializadas al mejor postor.

3. ¿Consideras que las entidades financieras te brindan información clara sobre tus derechos en cuanto a la protección de tus datos?

No, ninguna.

4. ¿Crees que las políticas de privacidad de las entidades financieras son claras y accesibles?

No.

5. ¿Alguna vez has sentido que tu información fue compartida con terceros sin tu consentimiento?

Sí, me pasó que durante el proceso de cobro, varias veces me llamaban a números de familiares. Me pareció que compartieron información personal sin mi consentimiento. Eso me afectó porque siento que mi privacidad fue vulnerada. No me sentí cómodo, y me dio la sensación de que todos sabían de mi situación financiera, lo cual es muy incómodo

3. INFORMANTE TRES

1. ¿Qué entiendes por protección de datos personales en el contexto financiero?

Salvaguardar la información sensible de los usuarios o cuentahabientes, que podrían ser usados con fines ilegales como la extorsión o la estafa.

2. ¿Alguna vez has sentido que tu información personal ha sido utilizada sin tu consentimiento por una entidad financiera?

En varias ocasiones, he recibido llamadas para ofrecer servicios financieros sin mi consentimiento.

El hecho de que entidades financieras a las cuales no he solicitado servicios ni proporcionado mis datos personales se contacten conmigo, podría ser un indicador de la difusión no consentida de información sensible entre dichas entidades.

3. ¿Consideras que las entidades financieras te brindan información clara sobre tus derechos en cuanto a la protección de tus datos?

No existe información específica sobre este tema, al menos en los medios convencionales.

4. ¿Crees que las políticas de privacidad de las entidades financieras son claras y accesibles?

Se encuentra disponible esta información en los canales virtuales, pero no está muy difundida actualmente.

5. Al momento del cobro de deudas, ¿Has sentido que tus datos con revelados? ¿ Cómo afecta esto a tu privacidad?

No estoy seguro si mis datos fueron revelados, sí recibí llamadas y mensajes de empresas de cobranza con información bastante específica sobre mi deuda. Esto me preocupa porque no sé cuántas personas tienen acceso a esa información. Siento que mi privacidad está en riesgo, ya que no debería ser tan fácil para cualquier empresa acceder a mis datos personales.

4. INFORMANTE SUPERINTENDENCIA DE BANCOS

1. ¿Cómo se supervisa el uso y tratamiento de los datos personales por parte de las entidades financieras?

La Superintendencia de Bancos enmarca su accionar en las funciones que determina el art. 62 del Código Orgánico Monetario y Financiero, de las cuales puedo resaltar 2 que están relacionadas al asunto en mención.

Numeral 16, respecto a proteger los derechos de los usuarios; y

Numeral 17, respecto a establecer clausulas obligatorias y las prohibiciones de los contratos de prestación de servicios financieros.

A su vez, el art. 352 del Código Orgánico Monetario y Financiero precisa claramente la protección de la información que tienen los usuarios financieros de forma general.

"Art. 352.- Protección de la información. Los datos de carácter personal de los usuarios del sistema financiero nacional que reposan en las entidades de dicho sistema y su acceso están protegidos, y solo podrán ser entregados a su titular o a quien éste autorice o por disposición de este Código."

Respecto a la protección de la información respecto al Registro de Datos Crediticios, el art. 360 del Código establece la obligatoriedad de guardar confidencialidad de la información, así como la prohibición de comercialización de información y responsabilidades.

Dentro de las acciones de control que efectúa la Superintendencia de Bancos, existen supervisiones extra situ e in situ las cuales tienen el fin de velar que las entidades sujetas a control cumplan debidamente con la normativa de su competencia, así como de emitir sanciones en caso de que se evidencien incumplimientos.

Actualmente las entidades del sistema financiero se encuentran ejecutando actualizaciones de los contratos de cuentas de ahorro, corrientes, tarjetas de crédito, etc, con el fin deadaptar el marco legal de la Ley Orgánica de Protección de Datos Personales.

Adicionalmente, la Superintendencia de Bancos tiene habilitados los canales de consultas, quejas y reclamos en los cuales usuarios pueden denunciar o comentar si se sienten afectados respecto al cumplimiento que dan las entidades financieras sobre sus datos personales.

2. ¿Cómo planea colaborar la Superintendencia con la nueva superintendencia de datos?

La Superintendencia de Bancos colaborará con los demás Organismos de Control según lo establece el art. 28 del Código Orgánico Administrativo, el cual menciona:

"Artículo 28.- Principio de colaboración. Las administraciones trabajarán de manera coordinada, complementaria y prestándose auxilio mutuo. Acordarán mecanismos de coordinación para la gestión de sus competencias y el uso eficiente de los recursos.

La asistencia requerida solo podrá negarse cuando la administración pública de la que se solicita no esté expresamente facultada para prestarla, no disponga de medios suficientes para ello o cuando, de hacerlo, causaría un perjuicio grave a los intereses cuya tutela tiene encomendada o al cumplimiento de sus propias funciones.

Las administraciones podrán colaborar para aquellas ejecuciones de sus actos que deban realizarse fuera de sus respectivos ámbitos territoriales de competencia. En las relaciones entre las distintas administraciones públicas, el contenido del deber de colaboración se desarrolla a través de los instrumentos y procedimientos, que de manera común y voluntaria, establezcan entre ellas."

3. ¿Cómo balancea la Superintendencia la necesidad de acceso a datos financieros, con la protección y el derecho a la privacidad de los usuarios?

Los derechos que tienen los usuarios se deben respetar en todo sentido. Como tal, es necesario que los Organismos de Control efectúen todas las acciones de control y actúen con las facultades que les permite la normativa vigente para precautelar que no se estén violentando los mismos y regular cualquier actividad improcedente.

Para esto, las entidades del sistema financiero nacional deben respetar el sigilo y reserva estipulado en el art. 353. del Código Orgánico Monetario y Financiero, a su vez todas las personas naturales y jurídicas deben acatar lo mencionado en el art. 355 respecto a la no divulgación de información, sin perjuicio de las sanciones y responsabilidad penal respectiva.

4. ¿Qué mecanismos existen para que los usuarios financieros puedan reportar vulneraciones a su privacidad?

En la actualidad existen canales virtuales y presenciales para los ingresos de quejas, consultas y reclamos y atención al usuario en general. A su vez, los usuarios pueden interactuar con la Superintendencia a través de redes sociales y los canales oficiales de la entidad.

Es importante recalcar que también dentro de cada entidad financiera, existe un Defensor del Cliente, quien es un facilitador y solucionador de conflictos entre las partes y que sus servicios no tienen ningún costo para el reclamante. La información de los medios de atención se puede visualizar a través del portal web www.superbancos.gob.ec