PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
SEDE MANABÍ
CARRERA DE DERECHO

TRABAJO DE TITULACIÓN

LA PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR Y SU LEGISLACIÓN APLICABLE EN ENTIDADES FINANCIERAS: UNA REFERENCIA AL EVENTO PÚBLICO BANCO PICHINCHA (2021)

LÍNEA DE INVESTIGACIÓN
DERECHO, PARTICIPACIÓN, GOBERNANZA, REGÍMENES POLÍTICOS E INSTITUCIONALIDAD

SUBLLÍNEA DE INVESTIGACIÓN
TRANSPARENCIA, RENDICIÓN DE CUENTAS Y DERECHOS CIUDADANOS

PREVIO AL TÍTULO DE
ABOGADO

AUTOR
JAIME ROBERTO HIDALGO SUAREZ

TUTOR
AB. LUIS ANGEL JARA PULLAS, MG.

PORTOVIEJO, ENERO 2024

Certificación del Tutor de Trabajo de Integración Curricular

Luis Ángel Jara Pullas, docente la Pontificia Universidad Católica del Ecuador Sede Manabí.

CERTIFICO:

En mi calidad de tutor del Trabajo de Integración Curricular, certifico haber revisado el presente manuscrito de investigación, el cual que se ajusta a las normas vigentes de la Pontificia Universidad Católica del Ecuador Sede Manabí, cumpliendo la Normativa del Trabajo de Integración Curricular; en consecuencia, es apto para su presentación y sustentación.

Portoviejo, 5 de enero de 2024

Atentamente,

Firmado electrónicamente por:
LUIS ANGEL JARA PULLAS

Luis Ángel Jara Pullas

Acta de Aprobación del Trabajo de Integración Curricular

El Tribunal examinador aprueba el Trabajo de Integración Curricular titulado “LA PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR Y SU LEGISLACIÓN APLICABLE EN ENTIDADES FINANCIERAS: UNA REFERENCIA AL EVENTO PÚBLICO BANCO PICHINCHA (2021)” en nombre de la Pontificia Universidad Católica del Ecuador Sede Manabí.

Firmado electrónicamente por:
LUIS ANGEL JARA PULLAS

Abg. Luis Ángel Jara Pullas, Mg.
Lector 1/Tutor

CARLA GUADALUPE GENDE RUPERTI

Digitally signed by CARLA GUADALUPE GENDE RUPERTI
DN: cn=CARLA GUADALUPE GENDE RUPERTI, serialNumber=0203221558 41, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, o=SECURITY DATA S.A. 2, c=EC
Date: 2024.01.26 13:58:53 -05'00'

Abg. Carla Guadalupe Gende Ruperti, Mg.
Lector 2

Abg. Gustavo Eduardo Briones Hidrovo, Mg.
Lector 3

Declaración de Originalidad

Este manuscrito no contiene ningún tipo de material que ha sido aceptado para la obtención de un título universitario en otra institución, excepto en forma de información de soporte que ha sido debidamente citada. Este trabajo es de total responsabilidad del autor, quien declara bajo juramento que ninguna sección de este trabajo de integración curricular infringe los derechos de otros autores.

Portoviejo, 5 enero de 2024

JAIME ROBERTO HIDALGO SUAREZ

Firmado digitalmente por JAIME ROBERTO HIDALGO SUAREZ
Fecha: 2024.01.05 14:38:00 -05'00'

Hidalgo Suarez Jaime Roberto

1312158791

Declaración sobre Derechos de Autor

Autorizo a la Pontificia Universidad Católica del Ecuador a distribuir este manuscrito de investigación en medios físicos y electrónicos con el fin de promover la divulgación de mis resultados a la comunidad científica y a la sociedad en general. Adicionalmente, autorizo el uso de los contenidos de esta investigación como bibliografía para fines académicos, por cualquier medio o procedimiento, citando como fuente al autor de este trabajo.

Portoviejo, 5 de enero de 2024

JAIME ROBERTO HIDALGO SUAREZ

Firmado digitalmente por JAIME ROBERTO HIDALGO SUAREZ
Fecha: 2024.01.05 14:38:14 -05'00'

Hidalgo Suarez Jaime Roberto

1312158791

Aprobación de Defensa Oral Pública

Los miembros del Tribunal designados por el honorable Comité Académico dan por aprobado el Trabajo de Titulación “LA PROTECCIÓN DE DATOS PERSONALES EN EL ECUADOR Y SU LEGISLACIÓN APLICABLE EN ENTIDADES FINANCIERAS: UNA REFERENCIA AL EVENTO PÚBLICO BANCO PICHINCHA (2021)”**.**

Abg. Luis Ángel Jara Pullas, Mg.	Abg. Carla Guadalupe Gende Ruperti, Mg.	Abg. Gustavo Eduardo Briones Hidrovo, Mg.
Tribunal 1/Tutor	**Tribunal 2**	**Tribunal 3**

A**gradecimiento**

Quiero expresar mi sincero agradecimiento por el apoyo incondicional que recibí durante la realización de mi trabajo de tesis. En primer lugar, agradezco a Dios por darme la fuerza y la determinación para llevar a cabo este proyecto académico.

A mis queridos padres, Jaime Hidalgo Marazita y María Luisa Suarez, les agradezco por su constante apoyo emocional, financiero y moral a lo largo de esta travesía académica. Sin su amor y aliento, este logro no habría sido posible.

A mi hermano Mario Hidalgo, quien me ha acompañado en cada paso de mi carrera, le agradezco su amistad, consejo y motivación. Tu presencia ha sido fundamental en mi camino hacia la graduación.

A Anette Núñez, agradezco su valiosa orientación y apoyo durante la etapa de tesis. Sus conocimientos y guía fueron fundamentales para el desarrollo de mi investigación.

Finalmente, a mi hermano Javier Espinoza, le agradezco por ser mi guía constante a lo largo de toda mi carrera académica. Tus consejos y sabiduría han sido un faro en mi camino hacia el éxito. A todos ustedes, les estoy profundamente agradecido por haber sido parte de este viaje y por su contribución a mi logro académico. Sin su apoyo, este trabajo de tesis no habría sido posible.

¡Gracias de todo corazón!

Dedicatoria

Dedico este trabajo de tesis con profundo cariño y gratitud a mis padres, Jaime Hidalgo Marazita y María Luisa Suarez, quienes han sido mi fuente constante de inspiración y apoyo a lo largo de mi vida académica. A todos mis hermanos, cuya presencia y ánimo han sido un pilar fundamental en mi camino hacia la graduación.

Agradezco a mis amigos más cercanos, quienes han estado a mi lado en cada paso de este viaje, brindándome su amistad y aliento incondicional hasta el día de hoy.

A mi abuela Elena Marazita, aunque ya no está físicamente presente, la llevo en mi memoria y corazón. Su amor y sabiduría siguen siendo una fuente de inspiración para mí.

Dieses Promotionsprojekt widme ich mit besonderer Hingabe meiner zweiten Familie in Österreich, Susi Wildzeiss und Herbert Wildzeiss, die ich immer in meinem Herzen trage.

Resumen

La presente investigación cualitativa analizó la protección de datos personales en el sector financiero, explorando la relación entre ambas variables en el contexto de la digitalización, destacando la importancia de equilibrar la innovación financiera preservando la privacidad. Por consiguiente, este estudio descriptivo ejecutado durante el 2023 analizó la aplicación de la normativa legal en el Banco Pichincha, comparándola con los casos de los bancos Santander y CaixaBank. Se realizó un análisis socio-jurídico a partir de dicha normativa y de los comunicados oficiales del Banco Pichincha, y se analizaron las declaraciones de sus usuarios realizadas a medios de comunicación considerando sus percepciones sobre la protección de datos. Los resultados indican que la Ley Orgánica de Protección de Datos (LOPD) en Ecuador regula el tratamiento de información mediante los principios de juridicidad, transparencia, finalidad, pertinencia, minimización de datos personales y confidencialidad, asegurando así un uso responsable de esta información sensible. La comparación de las resoluciones legales establece que la filtración de datos del Banco Pichincha en relación con las dos instituciones financieras internacionales no fue sancionada debido a la ausencia de una entidad reguladora como es la Superintendencia de Protección de Datos Personales. Las percepciones de los usuarios demuestran preocupación por el uso y/o fin que puede darse a sus datos personales por parte de quienes tienen acceso a ellos. En conclusión, es necesario que exista una protección sólida mediante un ente regulador capaz de establecer medidas punitivas para aquellas instituciones que no garanticen la privacidad de sus datos a los usuarios.

Palabras clave: jurisprudencia, regulación, privacidad, protección de datos personales, sector financiero

ABSTRACT

This qualitative research paper assessed personal data protection in the financial sector, by exploring the relationship between both variables in the digitalization context and emphasizing the importance of balancing financial innovation, while preserving data privacy. Therefore, this descriptive research study was conducted in 2023, and it analyzed the application of financial regulations in Banco Pichincha, by comparing it with the cases of Banco Santander and CaixaBank. A socio-legal analysis of these regulations and official communication from Banco Pichincha was carried out, and some user statements on their perceptions of data protection made to the media were analyzed. The findings reveal that the Organic Law on Protection of Personal Data (LOPD, for its initials in Spanish) in Ecuador regulates matters relating to the processing of personal data based on the principles of lawfulness, transparency, purpose limitation, relevance, data minimization, and confidentiality to ensure confidentiality of sensitive information. The comparison findings among financial regulations show that the data leak of Banco Pichincha was not subject to sanctions because there is not any regulatory entity such as the Superintendency of Personal Data Protection, as occurred in the other two international banks. The findings from the users' perceptions demonstrate their concern regarding the use and/or purpose that may be given to their personal data on behalf of those who have access to them. In conclusion, it is essential to develop solid data security protection provided by a regulatory body that imposes punitive measures against all those institutions that do not ensure customer data privacy.

Keywords: jurisprudence, regulation, privacy, personal data protection, financial sector

Índice

Introducción

En la era de la transformación digital, donde la información fluye a velocidades vertiginosas y las instituciones financieras se apoyan cada vez más en tecnologías avanzadas para brindar servicios eficientes, la protección de datos personales emerge como un imperativo crucial, la amalgama entre los datos personales y el sector financiero ha reconfigurado la manera en que concebimos tanto los derechos individuales como las responsabilidades de las instituciones financieras. En base a lo expuesto, la investigación propuesta tiene como punto de partida la necesidad imperante de comprender y abordar la protección de datos personales en el sector financiero, en un contexto marcado por la transformación digital y la rápida evolución de las tecnologías. Este estudio surge de la creciente relevancia de equilibrar la innovación financiera con la salvaguardia de la privacidad individual, siendo esta una preocupación central en la era contemporánea.

La problemática de la presente investigación se fundamenta en la acelerada digitalización de los servicios financieros, misma que requiere de manera urgente una contextualizada y eficiente regulación que garantice una adecuada protección de los datos personales. En este sentido, se plantea la siguiente pregunta de investigación: ¿Cuál es el marco normativo nacional que regula la protección de datos personales en las instituciones financieras en Ecuador? Para comprender el alcance de esta problemática, es necesario contextualizarla dentro del marco legal y normativo ecuatoriano. En este contexto, se examinan las regulaciones que rigen la protección de datos en el ámbito financiero, considerando la Ley Orgánica de Protección de Datos Personales y las instituciones financieras nacionales como elementos clave en la ecuación, de manera complementaria, se recurre a un análisis comparativo entre las regulaciones de Ecuador, México y Estados Unidos, explorando los matices y convergencias que moldean las obligaciones

de las instituciones financieras en cada jurisdicción. Además, se destaca la influencia de las normativas internacionales, en particular el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, en la definición de estándares y principios globales para la gestión de datos personales.

Como primer objetivo específico, se aborda la necesidad de examinar un marco teórico que permita comprender la relación entre los avances tecnológicos y la digitalización de la información en la sociedad actual. Este análisis teórico proporcionará el fundamento necesario para contextualizar la protección de datos personales en el entorno financiero.

La infracción tangible del derecho a la protección de los datos personales en el contexto de las instituciones financieras en Ecuador podría tener repercusiones significativas para los usuarios debido a que dichos datos constituyen información delicada que podría ser aprovechada de manera indebida con el propósito de llevar a cabo estafas, robo de identidad o actividades comerciales indeseadas, por lo cual como dentro de los objetivos específicos se busca identificar los derechos involucrados en la protección de datos personales según lo establecido en la Ley Orgánica de Protección de Datos Personales. Este objetivo específico permitirá desglosar los aspectos legales que sustentan la protección de la privacidad en el ámbito financiero ecuatoriano. De manera similar, conocer el procedimiento administrativo de control estatal para la protección de datos personales que se debe aplicar en colaboración con las instituciones financieras es crucial para entender cómo se implementa la regulación y cómo se supervisan y controlan las prácticas de protección de datos en el contexto financiero.

En base a lo expuesto, la presente investigación se erige como una brújula en la bruma de la protección de datos personales en el sector financiero y a medida que los capítulos se entrelazan, se busca tejer una narrativa completa que explore las complejas intersecciones entre

la innovación financiera, la protección de datos y las normativas legales.

Presentación del Problema Jurídico

La falta de aplicabilidad de la norma sobre la protección de datos personales por parte de las instituciones financieras produce la vulnerabilidad del derecho a protección de datos personales sea por acción u omisión, tal es el caso que desde que la normativa fue publicada en el registro oficial y entró en vigencia, meses después se cometió un ataque en donde estaba de por medio la institución financiera Banco de Pichincha, esto nos lleva a inferir la falta de aplicabilidad de la normativa destinada a la protección de datos personales.

En la actualidad, existe una problemática en cuanto a la falta de aplicabilidad de la normativa de protección de datos personales en las instituciones financieras en Ecuador, como es el caso de las instituciones financieras. Esta falta de cumplimiento de la normativa puede deberse a diversas razones, entre ellas la falta de conocimiento de las empresas financieras respecto a las obligaciones que tienen en cuanto al tratamiento de datos personales, así como a la falta de medidas disuasorias y sanciones efectivas por parte de las autoridades encargadas de hacer cumplir la normativa.

La vulneración material del derecho de protección de datos personales en las instituciones financieras en Ecuador puede afectar seriamente a los usuarios, ya que estos datos son información sensible que puede ser utilizada de manera ilícita para cometer fraudes, robo de identidad, o para fines comerciales no deseados. Los usuarios pueden experimentar una invasión a su privacidad, pérdida de control sobre sus datos personales y una vulnerabilidad ante posibles riesgos de seguridad y de usurpación de identidad. Además, al no poder ejercer sus derechos de acceso, rectificación, oposición y cancelación, los usuarios no podrán controlar cómo se procesa y almacena su información personal y financiera, lo que puede tener consecuencias negativas en

su bienestar y calidad de vida. Es fundamental que las instituciones financieras en Ecuador respeten y cumplan con las normas de protección de datos personales para garantizar el derecho fundamental de los usuarios a la privacidad y a la protección de su información personal.

Como resultado, de lo mencionado anteriormente los usuarios de las instituciones financieras pueden verse expuestos a la exposición no autorizada de sus datos personales, lo que puede tener graves consecuencias para la privacidad y seguridad de los ciudadanos. La falta de aplicación de la normativa de protección de datos personales en las instituciones financieras del Ecuador podría vulnerar materialmente el derecho de los usuarios a la protección de sus datos personales. Esta situación produciría consecuencias negativas para los titulares de los datos personales, como el uso indebido o la divulgación no autorizada de su información personal y financiera, lo que podría generar perjuicios económicos y sociales. Además, la falta de aplicación de la normativa podría limitar el control y la gestión que los usuarios tienen sobre sus propios datos personales, impidiéndoles conocer y decidir cómo se recopila, utiliza y almacena su información por parte de las instituciones financieras. Por tanto, es fundamental garantizar que las instituciones financieras cumplan con las obligaciones de la normativa de protección de datos personales para asegurar la protección de los derechos de los usuarios y evitar posibles perjuicios económicos y sociales.

Objetivos

Objetivo General

Investigar el marco normativo nacional aplicable para la protección de datos personales en las instituciones financieras.

Objetivos Específicos

- Examinar un marco teórico que permita comprender la relación entre los avances tecnológicos y la digitalización de la información de la información en la sociedad actual.
- Identificar los derechos involucrados en la protección de datos personales establecida en la Ley Orgánica de Protección de Datos Personales.
- Conocer el procedimiento administrativo de control estatal para la protección de datos personales que se debe aplicar con las instituciones financieras.

Aportes y valor de la investigación

En la última década ha surgido un cambio radical en la era digital, esto de la mano con las nuevas tecnologías que están ligadas al humano y a su vida diaria, dentro de todo esto se encuentra de por medio los datos personales, aquellos elementos que nos caracterizan y nos hacen identificables, incluso predecibles, como son nombres, apellidos, direcciones, teléfonos, actividad comercial, gustos musicales, preferencias políticas, inclinación religiosas, orientación sexual, entre otros, todos estos datos deben de ser protegidos y por ninguna situación deberían ser usados por terceras personas o empresas, para un fin que no sea el que se le haya mencionado al usuario que los proporciona, deben además ser tratados con suma delicadeza y en su debido momento ser eliminados de la base de datos en la que se almacenó para que evitar filtraciones.

La importancia de la protección de datos radica no solo en un tema de privacidad e intimidad, sino en un derecho constitucional reconocido en el 2008 en la constitución actual del Ecuador, las personas o empresas que manejen datos personales deben acarrear con un sentido de responsabilidad de toda esa información de sus usuarios, y la ley debe respaldar a las personas y el derecho a la no vulneración de sus datos personales.

Es así como se plantea demostrar en este proyecto es que en el Ecuador a pesar existir

una normativa vigente, se superpone la falta de aplicabilidad de la norma como una limitación para el ejercicio de la misma en el contexto de las instituciones financieras.

Por eso, es un desafío para el Ecuador poder llevar a cabo de manera correcta la ley de Protección de Datos, motivo por el cual este trabajo se proyecta a ayudar a la concientización de la protección de datos personales.

Capítulo I: Marco teórico - doctrinario

La protección de datos personales como derecho fundamental

Los datos personales comprenden aquellos elementos de información sensible que se asocian de manera particular con un individuo y que a su vez permiten a una persona ser identificada, por lo cual, debido a la intimidad inherente que significa su conocimiento, manejo o gestión surge el concepto de protección de datos, el mismo que la Comisión Económica para América Latina y el Caribe indica que abarca el derecho de las personas a estar informadas sobre qué datos están siendo recolectados y utilizados por terceros, ya sean organizaciones, empresas o entidades gubernamentales, incluyendo el derecho de corregir cualquier información inexacta o errónea que pueda existir en los registros (CEPAL, 2022). Así mismo, es un derecho novedoso, que surge a finales de los 70 como una medida destinada a resguardar el derecho a la intimidad de las personas, ya que el surgimiento de nuevas tecnologías que permiten el tratamiento masivo de datos demostró la necesidad de determinar un control sobre su uso (Fiallos, 2017).

La autora Conde Ortiz (2006) explica que el derecho a la protección de datos personales surge en base a la necesidad del amparo de los derechos de intimidad y de privacidad, manifestando que en el campo de la informática, especialmente en relación con el Estado, la persona que tiene el control sobre los datos que este maneja acerca de ella puede ejercer de manera más completa su libertad. Es así como se logra dimensionar el aspecto positivo de la intimidad, mismo que sienta sus bases en la doctrina y jurisprudencia de los Estados Unidos, que considera la *privacy* como el poder de ejercer un control sobre las informaciones que le atañen a uno, teoría que viene a considerar la intimidad como el derecho a poder participar y controlar las informaciones que conciernen a cada persona.

Así se sostiene que, aunque la protección de los datos personales está adecuadamente resguardada en las legislaciones modernas a través del derecho a la intimidad, es con la llegada de la informática, la capacidad de tratamiento automatizado de los datos y su transmisión, cuando surge una nueva relación entre los datos y las personas. En este contexto, el individuo requiere protección más allá de las normativas relacionadas con la intimidad. El derecho a preservar no se limita únicamente a la intimidad, sino que abarca un aspecto más profundo, conocido en los ordenamientos jurídicos anglosajones como "privacy" y que se ha traducido al castellano como "privacidad" (Conde Ortiz, 2006).

De acuerdo con la Asamblea Nacional del Ecuador (2021) en su documento titulado Ley Orgánica de Protección de Datos, estos son información que individualiza o permite la identificación de una persona física, ya sea de manera directa o indirecta, englobando cualquier dato relacionado o que pueda ser vinculado a una o varias personas físicas identificadas o identificables. En el proyecto de esta ley se mencionaba que corresponden entre otros a: nombre y apellido, fecha de nacimiento, dirección domiciliaria, correo electrónico, número de teléfono, número de cédula, matrícula vehicular, información patrimonial e información académica o cualquier otra información vinculada con la identidad del titular (Álvarez, 2017). Respecto al objetivo de la protección de datos personales, Núñez (2007) manifiesta:

> La protección de datos personales busca garantizar la privacidad de las personas el resguardo o protección de su intimidad, lo cual supone, fundamentalmente la posibilidad real de controlar el uso y la finalidad para la cual se destina la información relativa a los datos personales de cada individuo, y la facultad de oponerse a su utilización, de manera tal de impedir que esa información sirva a propósitos no aceptados por su titular (p. 114).

Es así, que los datos personales comprenden una forma de manifestación de varios derechos, como el derecho a la autodeterminación informativa, derecho a la intimidad, el derecho a la privacidad, lo que verifica que puede este ser considerado como un derecho fundamental.

Los derechos fundamentales son un conjunto de normas que protegen a los ciudadanos frente al Estado y limitan su poder. Estas normas se incluyen en la segunda categoría de normas que se encuentran en las Constituciones democráticas modernas. Los derechos fundamentales son derechos de elevadísima abstracción e importancia, en los cuales el objeto son determinadas posiciones del ciudadano descritas en abstracto (Carbonell & Alexy, 2013), por consecuente, son todos aquellos derechos subjetivos que corresponden universalmente a 'todos' los seres humanos en cuanto dotados del estatus de personas, de ciudadanos o de personas con capacidad de obrar (Ferrajoli, 2002).

El Tribunal Constitucional Español, al referirse al derecho de protección de datos personales en su Sentencia STC 292/2000 determina que el derecho fundamental a la protección de datos tiene como objetivo principal salvaguardar de manera efectiva la privacidad personal y familiar, a diferencia del derecho a la intimidad consagrado en el artículo 18.1 de la Constitución Española. No obstante, se distingue al otorgar a su titular un conjunto de facultades, principalmente en términos de poder jurídico, que le permiten exigir a terceros la realización o abstención de acciones específicas. La regulación precisa de estos poderes debe ser establecida por la ley, en conformidad con la disposición del artículo 18.4 de la Constitución Española, que limita el uso de la informática. Esta normativa puede ser desarrollada ya sea mediante la ampliación del derecho fundamental a la protección de datos (artículo 81.1 CE) o la administración de su ejercicio (artículo 53.1 CE). La singularidad de este derecho fundamental en comparación con el derecho a la intimidad radica en su función distintiva, lo que implica que

tanto su alcance como su contenido presenten diferencias significativas (Tribunal Constitucional de España, 2002). En este mismo contexto, Ordoñez (2019) afirma:

> Con la evolución de la tecnología, la sociedad ha experimentado gran dificultad para mantener protegidos algunos bienes jurídicos tradicionalmente tutelados a través del derecho a la intimidad, que ahora requieren una tutela más específica y amplia que les proporciona el derecho a la protección de datos personales o la autodeterminación informativa (p. 184).

De lo anterior se puede afirmar que, si bien el derecho a la protección de datos personales surgió como una forma de ampliar la protección de derechos como la intimidad y privacidad, actualmente es considerada como un derecho autónomo y procura protección y decisión sobre el uso de los datos personales, convirtiéndose además en un derecho fundamental.

Sánchez (2015) manifiesta que ante las capacidades tecnológicas para crear un "ciudadano transparente", surge la libertad informática, que se define como el "derecho a disponer de la información personal, a preservar la propia identidad digital o, en otras palabras, a consentir, controlar y corregir los datos informativos relativos a la propia personalidad". A la vez, se añade al derecho de informar y ser informado, el derecho de proteger la libertad de información como un bien personal.

Es así que este constituye un nuevo derecho fundamental cuyo propósito es otorgarnos el control que a cada uno de nosotros nos corresponde sobre la información que nos afecta a nivel personal (Botero, 2012), siendo que se verifica un derecho independiente que procura una protección necesaria sobre elementos que conforman su identidad, y que si bien tiene relación con otros derechos cumple una función concreta.

La protección de datos y su relevancia con las nuevas tecnologías y digitalización en la era digital

La gran revolución digital por la que ha atravesado el mundo especialmente a raíz de la pandemia mundial por COVID-19 ha marcado un antes y después respecto del uso de las nuevas tecnologías, de acuerdo con el Instituto Nacional de Estadísticas y Censos: “hasta el año 2022 un 69.7% de la población utilizaban internet” (INEC, 2022), cifra que seguramente continuará aumentando por la digitalización del diario vivir. En la era digital actual, la protección de datos se ha convertido en un tema de suma importancia debido al constante avance de las nuevas tecnologías y la creciente digitalización en todos los ámbitos de nuestra vida. La recopilación, procesamiento y almacenamiento masivo de información personal plantean desafíos significativos en términos de privacidad y seguridad.

Las tecnologías de información y comunicación, conocidas como TIC, han aportado, sin duda alguna, al desarrollo de las sociedades a través de la multiplicación del procesamiento y almacenamiento de datos en las relaciones cotidianas. Sin perjuicio de ello, y en contrapartida, no es posible desconocer los riesgos que, al mismo tiempo, aquellas han causado, relativos a la falta de seguridad de los datos personales. Esta situación ha generado el desarrollo de marcos normativos destinados a contrarrestar tales riesgos. Entre esta normativa, se encuentra aquella relativa al ámbito laboral (Blume, 2021).

La elaboración de perfiles se refiere a la recopilación y análisis de datos personales con el fin de crear perfiles detallados de individuos, lo que permite a las empresas y organizaciones comprender mejor los comportamientos, preferencias y necesidades de sus usuarios. Si bien esto puede ser útil para ofrecer productos y servicios personalizados, también plantea preocupaciones

en cuanto a la privacidad y la autonomía de los individuos. La información recopilada puede incluir datos sensibles y privados, como orientación política, preferencias sexuales o historial médico, lo que puede conducir a una violación de la intimidad si no se protege adecuadamente (Zambrano, 2022).

En este contexto, las leyes y regulaciones de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea o la Ley de Protección de Datos Personales en otros países, establecen requisitos específicos para garantizar que la elaboración de perfiles se realice de manera transparente y con el consentimiento del individuo. Estas leyes también establecen los derechos de los usuarios, como el derecho a acceder, rectificar o eliminar la información que se recopila sobre ellos. La implementación adecuada de estas medidas de protección de datos es esencial para equilibrar la innovación tecnológica con la privacidad y los derechos individuales (Herrera & Fandiño, 2020).

Además de la elaboración de perfiles, otro aspecto clave de la protección de datos en la era digital es el uso de cookies. Las cookies son pequeños archivos de texto que se almacenan en los dispositivos de los usuarios cuando visitan sitios web. Estas herramientas tecnológicas permiten a los sitios web recopilar información sobre el comportamiento de navegación de los usuarios y personalizar su experiencia en línea. Sin embargo, el uso de cookies también plantea preocupaciones en términos de privacidad y control de datos personales (CISP, 2016).

Las leyes de protección de datos establecen que los sitios web deben informar a los usuarios sobre el uso de cookies y obtener su consentimiento antes de almacenar o acceder a información en sus dispositivos. Además, los usuarios tienen derecho a configurar sus preferencias de cookies y pueden optar por no ser rastreados o limitar la recopilación de datos. Estas medidas son fundamentales para garantizar que los usuarios tengan control sobre su

información personal y puedan decidir cómo se utiliza y comparte. La protección de datos es un aspecto crucial en esta era digital, donde las nuevas tecnologías y la digitalización han transformado nuestra forma de vida. La elaboración de perfiles y el uso de cookies son solo dos ejemplos de cómo se recopila y procesa la información personal en línea. Es esencial contar con leyes y regulaciones sólidas que establezcan principios claros de protección de datos y garanticen que los individuos mantengan el control sobre su información personal. Además, es importante que los usuarios estén informados y ejerzan sus derechos en relación con la privacidad y la seguridad de sus datos en la era digital en constante evolución (Meyer, 2004).

Aspectos fundamentales de la protección de datos personales para usuarios de instituciones financieras privadas

Para asegurar el efectivo cumplimiento de la protección de datos personales, se han establecido principios reguladores del tratamiento de la información, los cuales se encuentran detallados en el artículo 10 de la Ley Orgánica de Protección de Datos Personales del Ecuador. Estos principios han sido incorporados en nuestra legislación, tomando como referencia el Reglamento General de Protección de Datos de la Unión Europea, el cual, en su artículo 5, ha marcado un estándar mundial en materia de protección de datos desde su entrada en vigor en 2018. Estos principios mencionados se encuentran en la Ley Orgánica de Protección de Datos elaborada por la Asamblea Nacional (2021) se indica:

> En relación con la juridicidad, la legislación aplicable y la jurisprudencia destaca la importancia de un enfoque legal y normativo en la protección de datos personales y establece en el literal (a) que “los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la constitución,

> los instrumentos internacionales, la presente Ley, su Reglamento y la demás normativa y jurisprudencia aplicable (Ley Orgánica de Protección de Datos, 2021, Art. 10).

Es decir, la necesidad de garantizar que el tratamiento de la información personal se ajuste a un marco jurídico sólido y coherente, en este sentido, la protección de datos se erige como un derecho fundamental, respaldado por la normativa nacional e internacional, que busca preservar la privacidad y la autonomía de los individuos, estableciendo la jurisprudencia como una herramienta dinámica para interpretar y adaptar las normas a los desafíos emergentes en la era digital.

El principio de lealtad en el tratamiento de datos personales constituye un pilar fundamental en la protección de la privacidad y la autonomía de los individuos. Esta exigencia implica que las entidades que manejan información personal deben ser transparentes en sus prácticas, garantizando que los titulares de los datos comprendan de manera clara y honesta cómo se recopilan, utilizan y tratan sus datos, tal como lo establece el literal (b) del artículo ya mencionado, donde consta que "el tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados" (Ley Orgánica de Protección de Datos, 2021, Art. 10). Este enfoque resuena con la noción de consentimiento informado, donde la toma de decisiones autónoma de los individuos se eleva como un principio rector, recordando que no solo es un requisito ético, sino también un mecanismo esencial para fortalecer la confianza entre las partes involucradas.

En el contexto de la protección de datos, el principio de transparencia desarrollado en el literal (c) implica que "el tratamiento de datos personales deberá ser transparente, por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de

entender y se deberá utilizar un lenguaje sencillo y claro" (Ley Orgánica de Protección de Datos, 2021, Art. 10). Para esto, las personas deben ser informadas de manera clara y comprensible sobre cómo se recopilan, procesan y utilizan sus datos personales y este enfoque no solo aboga por la divulgación de prácticas de manejo de datos, sino que también destaca la importancia de utilizar un lenguaje sencillo y accesible, en este sentido, la transparencia no solo se traduce en la divulgación de información, sino también en la comprensión efectiva por parte de los individuos afectados y se alinea con el principio de autonomía informativa, donde se reconoce la capacidad de los individuos para tomar decisiones informadas sobre el manejo de sus datos personales, por lo cual contribuye a un ejercicio efectivo de los derechos de privacidad por lo cual es esencial que la legislación y las prácticas empresariales se alineen con estos principios, fomentando la creación de un entorno digital donde la transparencia sea la piedra angular de la protección de datos personales (López, 2013).

El principio de finalidad, que corresponde al literal (d) destaca la necesidad de informar adecuadamente a los titulares de datos sobre el propósito específico para el cual se recaban sus datos, y establece que "las finalidades del tratamiento deberán ser (…) explícitas 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" (Ley Orgánica de Protección de Datos, 2021, Art. 10). Este enfoque no solo fortalece la confianza entre los usuarios y las entidades que gestionan la información, sino que también establece límites claros para evitar el uso indebido de datos personales, es así que se puede destacar que esta orientación se alinea con la noción de "finalidad específica" en el ámbito de la privacidad, donde la recopilación y procesamiento de datos deben limitarse a propósitos determinados y legítimos, además, este enfoque resuena con el principio de proporcionalidad, subrayando que la

recopilación de datos debe ser proporcionada al propósito previamente establecido (Ley Orgánica de Protección de Datos, 2021, Art. 10). En este sentido, la protección de datos personales no solo implica resguardar la privacidad individual, sino también preservar la integridad del individuo y la confianza en el uso responsable de la información personal (Chen Mok, 2010).

El principio de pertinencia y minimización de datos personales, reflejado en la afirmación de que la información debe ser "estrictamente necesaria para cumplir con la finalidad del tratamiento" (Ley Orgánica de Protección de Datos, 2021, Art. 10), como se expone en el literal

> (e) del artículo ya mencionado constituye un pilar fundamental en la protección de datos, desde una perspectiva doctrinaria, este enfoque se alinea con el principio de proporcionalidad, que busca equilibrar la necesidad de recopilar información con la preservación de la privacidad y la limitación de los riesgos asociados al procesamiento de datos. Este principio encuentra su sustento en el respeto a la autodeterminación informativa, reconociendo la importancia de que los individuos tengan control sobre la cantidad y naturaleza de la información personal que comparten. Además, su aplicación promueve la transparencia y la confianza en las relaciones entre los titulares de datos y los responsables del tratamiento (Fiallos, 2017).

En relación con la proporcionalidad del tratamiento de datos, implica que “el tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos” (Ley Orgánica de Protección de datos, 2021, Art. 10) evitando la obtención de datos superfluos o irrelevantes, esta necesidad resalta la importancia de limitar el tratamiento a lo esencial, evitando la acumulación excesiva de información, señalando la relevancia de realizar el tratamiento en el momento adecuado, sin dilaciones innecesarias. Por

último, destaca la importancia de que los datos tratados guarden una relación directa con los propósitos previamente definidos. Este enfoque proporcional no solo respalda la eficacia de las operaciones de tratamiento, sino que también salvaguarda la privacidad individual, especialmente en el caso de categorías especiales de datos, donde la prudencia y restricción adicional son cruciales (Aguilar Guzmán et al., 2022).

La confidencialidad impone a los responsables del tratamiento la responsabilidad de garantizar la seguridad y confidencialidad de los datos, debido a que "debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos" (Ley Orgánica de Protección de datos, 2021, Art. 10). Así mismo, la mención de causales legítimas que permitan el tratamiento o divulgación de datos para fines distintos establece un equilibrio necesario entre la protección de la privacidad y las situaciones excepcionales en las que se justifica una utilización diferente de la información. En este sentido, la doctrina reconoce la necesidad de establecer normativas claras que definan y limiten las excepciones permitidas, garantizando así la coherencia y la legalidad en el manejo de datos personales (Carrillo, 2021).

Desde una perspectiva doctrinaria, la calidad y exactitud de los datos establece que "deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados" (Ley Orgánica de Protección de datos, 2021, Art. 10), por lo cual se alinea con la noción de autodeterminación informativa, donde los individuos tienen el derecho de controlar la información personal que se recopila sobre ellos, la obligación de suprimir o rectificar datos inexactos refleja la preocupación por evitar la manipulación indebida de la información, lo que está en sintonía con las regulaciones de protección de datos a nivel internacional (Aguilar Guzmán et al., 2022).

El principio de conservación de datos personales destaca la importancia de limitar el tiempo de retención de la información personal en lo estrictamente necesario para cumplir con la finalidad del tratamiento y menciona que “serán conservados durante un tiempo no mayor a 30 días, para cumplir con la finalidad de su tratamiento” (Ley Orgánica de Protección de datos, 2021, Art. 10). Esta premisa subraya la necesidad de que los responsables del tratamiento establezcan plazos definidos para la supresión o revisión periódica de los datos, con el propósito de evitar la conservación innecesaria de información sensible (AEPD, 2021). De esta manera, la implementación efectiva de plazos de retención específicos no solo cumple con la normativa vigente, sino que también contribuye a fortalecer la confianza de los individuos en el manejo responsable de sus datos personales.

En relación con el principio de seguridad de los datos personales se basa la evolución dinámica de las amenazas cibernéticas y la creciente conciencia sobre la importancia de la privacidad individual y establece que se “deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica (…) para proteger los datos personales frente a cualquier riesgo” (Ley Orgánica de Protección de datos, 2021, Art. 10). De esta manera se puede apreciar la convergencia con principios como el de proporcionalidad y el enfoque basado en riesgos, promoviendo así la implementación de medidas de seguridad que no solo sean eficaces, sino también contextualmente relevantes.

El principio de responsabilidad proactiva y demostrada impone una carga adicional al responsable del tratamiento de datos, exigiéndole no solo el cumplimiento normativo, sino también la evidencia concreta de la implementación de mecanismos de protección adecuados, es decir, la evolución hacia un paradigma más robusto en materia de privacidad, instando a las organizaciones a adoptar una postura proactiva en la salvaguarda de la información personal

(Ley Orgánica de Protección de datos, 2021, Art. 10). En este contexto, la doctrina aboga por la integración de estándares y mejores prácticas como elementos fundamentales para garantizar una protección efectiva.

El principio de aplicación favorable al titular se alinea con la esencia misma de la normativa de privacidad, que busca salvaguardar los derechos fundamentales de los individuos, al adoptar una posición proactiva hacia la protección de la privacidad, se reconoce la importancia intrínseca de preservar la autonomía y la intimidad de las personas y menciona que " en caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico (…), los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos" (Ley Orgánica de Protección de datos, 2021, Art. 10). Es decir, refleja la necesidad de superar posibles ambigüedades o lagunas normativas en favor de la protección del titular de los datos y contribuye a la construcción de una cultura de respeto y salvaguarda de la información personal en la sociedad.

El principio de independencia del control garantiza que la autoridad pueda actuar de manera objetiva y sin interferencias externas, lo que fortalece la confianza de los individuos en el manejo adecuado de su información personal y confiere a la autoridad un papel proactivo en la salvaguarda de la privacidad lo cual se expresa en el literal (m) y menciona que " la Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción" (Ley Orgánica de Protección de datos, 2021, Art. 10). Esto permite abordar posibles vulneraciones de manera oportuna y eficaz, motivo por el cual, se destaca la importancia de establecer marcos regulatorios que fortalezcan la independencia de las autoridades de protección de datos, contribuyendo así a la construcción de un entorno digital más seguro y respetuoso de los derechos individuales.

Es así, que los principios de la protección de datos personales establecen un marco ético y legal para el tratamiento adecuado de la información personal. Estos principios se desarrollan con el propósito de garantizar la privacidad, seguridad y control de los individuos sobre sus datos personales en el contexto digital. Estos principios existen para salvaguardar los derechos de privacidad de los individuos y establecer límites y responsabilidades para aquellos que manejan datos personales. Buscan equilibrar el uso legítimo de la información con la protección de la privacidad y la seguridad de los datos, asegurando que el tratamiento de datos personales se realice de manera ética, transparente y responsable. Estos principios están interconectados y, al mismo tiempo, tienen en cuenta la visión horizontal del género y los derechos humanos para determinar el impacto diferenciado del procesamiento de datos y resolver la situación con una fragilidad especial (Comité Jurídico Interamericano, 2021).

Es así como implementar medidas de seguridad, documentarlas y mantenerlas no solo busca reducir el impacto económico derivado de posibles sanciones de la autoridad, sino que también conlleva beneficios significativos en la era digital, donde la protección de datos se vuelve crucial. Más allá de las implicaciones financieras, el establecimiento de estas medidas contribuye de manera fundamental al fortalecimiento de la certidumbre y confianza de los titulares de datos personales. En un entorno donde la privacidad digital es una preocupación creciente, generar confianza se convierte en un activo estratégico (Carrillo, 2021). Además, este enfoque proactivo no solo se traduce en el cumplimiento de las normativas, sino que también refuerza la competitividad del mercado al elevar los estándares de seguridad.

Mejorar los procesos internos de la organización y su eficiencia se convierte en un subproducto beneficioso, lo que no solo optimiza la gestión de datos, sino que también favorece la adaptación a un entorno digital en constante evolución. La inversión, incluso desde

perspectivas internacionales, se ve facilitada por la confianza en la integridad y protección de los datos, impulsando así un flujo más libre y seguro de información en la era digital (INAI, 2015). En el artículo de Herrera & Fandiño (2020), el cual tiene como nombre “La Protección de Datos en la Era Digital” citan al abogado Recio, el cual manifiesta:

> La cantidad de información gestionada en distintos medios de almacenamiento tecnológico está en constante crecimiento, lo cual se refleja de manera notable en las estadísticas. En 2013, se calculaba que existían alrededor de 4.4 zettabytes de información de diversos tipos almacenados en plataformas digitales. En contraste, para el año 2020, se observa un aumento significativo, con una cifra estimada de 44 zettabytes de información circulando en diversas plataformas (p. 14).

Por lo cual, ante el inminente incremento de almacenamiento de datos a nivel digital, es crucial la implementación de medidas de seguridad, documentación y mantenimiento mismas que se alinea con principios clave de protección de datos, donde las organizaciones asumen la responsabilidad de garantizar la protección de los datos bajo su custodia.

Los derechos de los titulares en relación con la protección de datos personales constituyen un conjunto esencial de prerrogativas destinadas a preservar la privacidad y la autodeterminación de las personas en la era digital. Estos derechos reconocen la importancia de supervisar la información personal y prevenir su uso indebido, al mismo tiempo que fomentan la transparencia y la responsabilidad por parte de quienes recopilan y procesan datos. En la sociedad contemporánea, la protección de datos personales se ha vuelto central debido a la creciente recopilación y compartición de información en diversas áreas, desde transacciones en línea hasta la gestión de registros médicos. Estos derechos proporcionan un marco legal y ético crucial para asegurar que las personas puedan ejercer un control significativo sobre sus datos y

preservar su privacidad en un mundo cada vez más interconectado. Un componente fundamental de estos derechos es el derecho a la información, que implica la obligación de informar adecuadamente a los individuos sobre la recopilación, registro y propósito del uso de su información personal. Este derecho destaca la importancia de que las entidades o personas responsables del tratamiento de datos tengan políticas transparentes en relación con el manejo de datos personales (Pineda, 2019).

El derecho de acceso constituye una de las principales prerrogativas que forma parte integral de la protección de datos personales. Este derecho concede a los individuos la capacidad de supervisar la información personal almacenada por terceros, ya que, en principio, cualquier persona que lo solicite tiene el derecho de consultar la información que se ha registrado sobre ella en un archivo o base de datos, según lo estipulado por la legislación correspondiente. En consecuencia, reconocer el derecho de acceso habilita a los ciudadanos para acceder a los archivos o registros que contienen sus datos personales y obtener conocimiento sobre qué datos han sido objeto de tratamiento. Es importante señalar que este derecho no solo permite acceder a información específica relacionada con los datos personales bajo tratamiento, sino que también proporciona detalles sobre el origen de dichos datos, los propósitos de los tratamientos correspondientes y los destinatarios (García González, 2007).

El derecho de rectificación permite al individuo solicitar a la entidad responsable del archivo la enmienda de cualquier información personal que pueda estar incompleta o incorrecta. Normalmente, este derecho se ejerce después del derecho de acceso, ya que solo una vez que se ha ejercido este último, la persona podrá determinar si los datos tratados son imprecisos o faltantes. Este derecho de rectificación guarda una estrecha relación con el principio de calidad o veracidad de los datos, ya que ambos tienen como objetivo asegurar que el tratamiento de los

datos refleje con precisión la realidad (Aguilar Guzmán et al., 2022).

Uno de los pilares fundamentales dentro del manejo responsable de los datos personales es la potestad del usuario a requerir la eliminación o supresión de sus datos personales cuando el mismo sienta que se han incumplido los principios estipulados en las normativas vigentes, en relación con esta afirmación, la Asamblea Nacional (2021) en su documento titulado Ley Orgánica de Protección de Datos Personales menciona este derecho a la eliminación puede ser requerido bajo los siguientes parámetros:

> El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad; los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados; haya vencido el plazo de conservación de los datos personales; el tratamiento afecte derechos fundamentales o libertades individuales; revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o, exista obligación legal (Ley Orgánica de Protección de Datos, 2021, Art. 10).

El derecho de oposición otorga a la persona involucrada la capacidad de detener el procesamiento de sus datos personales cuando exista una razón legítima basada en su situación personal particular. La oposición implica que el tratamiento de los datos aún no se ha llevado a cabo, ya que, en el caso contrario, sería apropiado ejercer el derecho de cancelación (GOVERTIS, 2021).

Así mismo, el derecho a la portabilidad es un derecho que implica que la persona afectada tiene el derecho de recibir sus datos personales, que haya proporcionado a un responsable de procesamiento, en un formato estándar legible por máquinas y estructurado, y también tiene el derecho de transferirlos a otro responsable de procesamiento sin que el

responsable original lo impida. En caso de ser técnicamente viable, la persona afectada también tiene el derecho a que los datos personales se transmitan directamente de un responsable a otro (AEPD, 2023).

Así mismo, se debe recordar que, entre otros principios, el titular posee el derecho de no ser objeto de decisiones basadas exclusiva o parcialmente en evaluaciones generadas por procesos automatizados, incluyendo la creación de perfiles, que puedan tener consecuencias jurídicas o afectar sus derechos fundamentales y libertades. Además, se reconoce el derecho de consulta, permitiendo a las personas acceder de manera pública y gratuita al Registro Nacional de Protección de Datos Personales, de acuerdo con lo dispuesto en esta misma ley. De la misma manera, se garantiza el derecho a la educación digital, que implica el acceso y disponibilidad del conocimiento relacionado con el uso adecuado y responsable de las tecnologías de la información y comunicación. Este derecho, en conformidad con la Ley Orgánica de protección de datos, enfatiza la importancia de respetar la dignidad humana, los derechos fundamentales, y promover una cultura consciente en relación con la protección de datos personales (Ley Orgánica de Protección de Datos, 2021, Art. 23).

Términos y Obligaciones en Protección de Datos para Entidades Financieras en Ecuador: Cumplimiento, Sanciones y Actualizaciones Legales

En el sector financiero, las instituciones financieras y otras entidades relacionadas deben cumplir con las disposiciones establecidas en la LOPD y su reglamento. Estas normas exigen que se obtenga el consentimiento informado de los titulares de los datos antes de recopilar y procesar cualquier información personal. Además, se requiere que las entidades financieras adopten medidas de seguridad adecuadas para proteger los datos personales y eviten su acceso no

autorizado, pérdida o divulgación (González, 2021).

La LOPD también establece los derechos de los titulares de datos, como el acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales. Las entidades financieras deben implementar procedimientos internos para atender las solicitudes de los titulares de datos y asegurarse de que se respeten estos derechos (Ministerio de telecomunicaciones y de la sociedad de la información, 2019). Es así, que, en caso de incumplimiento de las disposiciones de protección de datos, las entidades financieras pueden enfrentar sanciones y responsabilidades legales. La Agencia de Regulación y Control de Datos Personales (ARCO) es la entidad encargada de supervisar y hacer cumplir las normas de protección de datos en Ecuador (Russel, 2023).

Es importante destacar que la legislación y los requisitos específicos pueden cambiar con el tiempo, por lo que es fundamental mantenerse actualizado sobre las leyes y regulaciones vigentes en Ecuador y buscar el asesoramiento de un abogado especializado en protección de datos y derecho financiero (Ramírez, 2023). Finalmente, el marco normativo de protección de datos en Ecuador, incluido en la Ley Orgánica de Protección de Datos establece los principios y reglas para el tratamiento de datos personales en el sector financiero, es así como las entidades financieras deben obtener el consentimiento informado, implementar medidas de seguridad adecuadas y respetar los derechos de los titulares de datos. El incumplimiento de estas normas puede dar lugar a sanciones y responsabilidades legales.

Capitulo II: Marco metodológico y/o jurisprudencial

Nuestro paradigma de investigación es la trilogía jurídica ya que combinamos la norma, el valor y la realidad. Se hace ciencia jurídica cuando se va más allá de la norma, contemplándose la realidad social. Galati (2021) establece que desde este paradigma se hace ciencia jurídica cuando se va más allá de la norma, contemplándose la realidad social.

Para el presente trabajo utilizaremos un tipo de investigación dogmática en el sentido de que se realizará una aproximación a la norma jurídica donde se pueda comprender la aplicación de la Ley Orgánica de Protección de Datos Personales (LOPDP) a las instituciones financieras privadas, con particular énfasis en un caso que gozó de publicidad a través de los medios de comunicación y que involucró a la institución financiera Banco Pichincha. En ese sentido, Tantaleán explica que hemos de utilizar "esta denominación por extensión a todo tipo de investigación cuyo basamento sean las normas jurídicas y siempre que se las analice de modo abstracto o teórico" (2016, p. 4). Por otra parte, también consideramos que esta investigación se circunscribe al tipo sociológico jurídico en razón de que nos orientamos a examinar los datos de la experiencia jurídica que la institución financiera Banco Pichincha implementa respecto de la aplicabilidad de la ley, es decir, se analizará "si la norma jurídica se cumple o no en la realidad, sin entrar a detallar su validez o su legitimidad" buscamos entonces "verificar la aplicación del derecho pero en sede real; por tanto, se trata de ir a la misma realidad, […]" (Tantaleán, 2016, p. 10).

El método que hemos aplicado a este trabajo es el inductivo tomando como referencia el caso particular de una institución financiera establecemos conclusiones generales. "La inducción como forma lógica de razonamiento es el proceso mental que partiendo de casos particulares llega a su causa o explicación que ha sido previamente formulada de manera general" (Clavijo et

al, 2014, p. 16). Así mismo hemos aplicado el método de análisis y síntesis entendido en los términos que plantean Clavijo et al (2014) separando las partes de un todo para analizarlas independientemente estableciendo diferentes relaciones y luego la reunión racional de dichos elementos para presentarlos como un todo.

Las fuentes que hemos utilizado para este trabajo de investigación son: primarias la ley y los instrumentos internacionales, la jurisprudencia; secundarias, la doctrina, textos especializados y el hecho social concreto (caso de la institución financiera). Nuestras técnicas de investigación han sido la revisión bibliográfica, la selección de información, el análisis de información, la sistematización de la información.

Marco Normativo y Protección De Datos Personales En El Sector Financiero

En Ecuador, la protección de datos personales está regulada por la Ley Orgánica de Protección de Datos Personales en adelante LOPD y su reglamento. Estas normativas establecen los principios y las reglas para el tratamiento de los datos personales y garantizan los derechos de los titulares de dichos datos. El artículo 1 de la Ley Orgánica de Protección de Datos Personales elaborado por la Asamblea Nacional (2011) nos habla sobre el objetivo y finalidad que tiene, el cual dice lo siguiente “El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela” (Ley Orgánica de Protección de datos, 2011, Art. 1).

La LOPD establece un conjunto de principios rectores, como el principio de consentimiento informado, que exige a las entidades financieras obtener la aprobación explícita

de los titulares de datos antes de recopilar y procesar su información personal. Este principio se convierte en el pilar sobre el cual se erige todo el procedimiento administrativo relacionado con la recopilación y uso de datos en el sector financiero. En relación con el procedimiento administrativo también se enfoca en la finalidad legítima y proporcionalidad en el tratamiento de datos personales. Esto implica que las entidades financieras deben definir claramente los propósitos para los cuales se recopilan los datos y limitar su uso a lo estrictamente necesario para alcanzar esos objetivos. Además, se destaca la obligación de adoptar medidas técnicas y organizativas adecuadas para proteger los datos contra pérdidas, accesos no autorizados o cualquier forma de procesamiento indebido, conforme al artículo 14 de la LOPD (Ordóñez Pineda et al., 2022).

En relación con los derechos de los titulares de datos, el procedimiento administrativo establece que las entidades financieras deben implementar mecanismos internos para atender solicitudes de acceso, rectificación, cancelación y oposición (ARCO). Este enfoque garantiza que los individuos tengan un control efectivo sobre su información personal y que las entidades financieras cumplan con las obligaciones legales en este ámbito (Redrobán Barreto, 2023).

No obstante, es crucial destacar que el procedimiento administrativo no solo se aplica a empresas privadas, sino también a entidades del sector público que manejan datos personales en el ámbito financiero. Esto refuerza la necesidad de una protección integral, independientemente de la naturaleza de la entidad que maneje dicha información.

Ley Comparada

Comparación entre México y Ecuador:

La Ley de Protección de Datos Personales en México es una legislación clave que busca salvaguardar la privacidad y seguridad de la información personal de los individuos. Esta ley,

también conocida como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, fue promulgada en 2010 y ha sido una pieza fundamental para regular el tratamiento de los datos personales en el país.

El objetivo principal de esta ley es garantizar que las empresas y organizaciones que recopilan utilizan o almacenan datos personales cumplan con ciertos estándares de seguridad y privacidad, de manera similar a Ecuador, la Ley de Protección de Datos Personales en México se basa en el derecho a la intimidad, lo que se vincula con la existencia de un ámbito privado reservado frente a la acción y conocimiento de terceros, ya sean individuos comunes o los Poderes del Estado. En este contexto, el artículo 45 de la Ley de Protección de Datos Personales en México menciona que cuando el responsable de la unidad administrativa haya designado como reservados o confidenciales los documentos solicitados para acceso, se debe de enviar una solicitud de información junto con un oficio que justifique y explique dicha clasificación al comité correspondiente de la dependencia o entidad de la administración pública. Este comité se encargará de determinar si confirma, modifica o revoca la clasificación con el fin de resguardar los datos personales en tratamiento (Suprema Corte de Justicia de la Nación, 2018).

Bajo esta legislación, se establece la obligación de las empresas de adoptar medidas técnicas y organizativas adecuadas para proteger los datos personales de posibles pérdidas, robos o accesos no autorizados. El artículo 14 de la Ley Federal de Protección de Datos Personales en México (2010) dice lo siguiente: “El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación…”. Es importante destacar que la Ley de Protección de Datos Personales en México no sólo se aplica a empresas y organizaciones privadas, sino también a entidades del sector público que manejan datos personales, esto garantiza una protección integral

de la información personal, independientemente de la entidad que la recopile o utilice. Sin embargo, a pesar de los avances logrados con esta ley, aún existen desafíos en su implementación efectiva. Algunas empresas y organizaciones pueden no estar plenamente conscientes de sus obligaciones o pueden incumplir con las medidas de seguridad necesarias. Además, el crecimiento tecnológico y la digitalización constante plantean nuevos retos en la protección de datos, lo que requiere una constante actualización y adaptación de la legislación (Cristea, 2017).

Ley de Protección de Datos Personales en Ecuador:

En Ecuador el nombre oficial de la ley es "Ley Orgánica de Protección de Datos Personales", esta ley tiene como propósito garantizar el ejercicio del derecho a la protección de los datos personales, así como regular su tratamiento por parte de personas naturales y jurídicas, tanto del sector público como privado. La autoridad que se encargan de regularla es "La Agencia de Regulación y Control de Datos Personales" (ARCO) es la entidad encargada de velar por el cumplimiento de esta ley. Entre los principios establecidos se incluyen el principio de consentimiento, finalidad legítima, calidad de los datos, proporcionalidad, seguridad, confidencialidad y transparencia. Los titulares de los datos tienen derechos similares a los de México, que incluyen el acceso, rectificación, cancelación y oposición (ARCO), así como el derecho a la portabilidad y la limitación del tratamiento de sus datos (Enríquez, 2018).

En la LOPD (2021), en el artículo 5 nos dice lo siguiente: "Son parte del sistema de protección de datos personales, los siguientes: titular; responsable del tratamiento; encargado del tratamiento; destinatario; autoridad de Protección de Datos Personales; y, delegado de protección de datos personales".

Es así la que Ley Federal de Protección de Datos Personales en México, promulgada en 2010, ha sido una pieza clave para garantizar la seguridad y privacidad de la información personal en el país. A través de principios fundamentales como el consentimiento informado, finalidad específica y proporcionalidad, la ley busca regular el manejo adecuado de los datos personales por parte de empresas y organizaciones, tanto del sector privado como público. Sin embargo, a pesar de los avances, persisten desafíos en su implementación efectiva, especialmente en un entorno digital en constante evolución (Gobierno de México, 2020). En Ecuador, la Ley Orgánica de Protección de Datos Personales cumple un papel similar, regulando el tratamiento de datos por parte de entidades públicas y privadas.

Comparación entre Estados Unidos y Ecuador:

La protección de datos personales en Estados Unidos se rige por un conjunto de leyes y regulaciones que buscan garantizar la privacidad y seguridad de la información personal de los individuos. Aunque no existe una única ley federal de protección de datos en Estados Unidos, existen varias leyes y regulaciones que abordan diferentes aspectos de la privacidad y protección de datos.

Una de las leyes más relevantes en este ámbito es la Ley de Privacidad de las Comunicaciones Electrónicas (Electronic Communications Privacy Act, ECPA) de 1986. Esta ley establece las normas para la interceptación y acceso a las comunicaciones electrónicas, así como la protección de la privacidad de los usuarios de servicios de comunicación electrónica (Bureau of Justice Assistance, 1986).

Además, la Ley de Protección de Información Personal y Documentos Electrónicos (Gramm-Leach-Bliley Act, GLBA) de 1999 es otra legislación importante en el ámbito de la

protección de datos en el sector financiero. Esta ley exige a las instituciones financieras que implementen medidas de seguridad y privacidad para proteger la información personal de los clientes (Organization of American States, 2012).

Es importante tener en cuenta que la protección de datos en Estados Unidos se basa en un enfoque sectorial y se encuentra en constante evolución. A medida que avanza la tecnología y las preocupaciones sobre la privacidad aumentan, se han propuesto y discutido varias iniciativas a nivel federal para fortalecer la protección de datos personales en el país. Tomando en cuenta lo anterior, la ley ecuatoriana establece principios como el consentimiento, finalidad legítima y seguridad, y otorga derechos a los titulares de los datos, incluyendo el acceso, rectificación, cancelación y oposición (ARCO), así como el derecho a la portabilidad y la limitación del tratamiento (Cámara de Industrias y Producción, 2023).

Sin embargo, la principal diferencia radica en que Ecuador cuenta con una ley de protección de datos personales a nivel nacional, mientras que, en los Estados Unidos, la regulación se centra en leyes sectoriales y estatales. Esto implica que, en los Estados Unidos, las regulaciones y requisitos pueden variar significativamente según el sector y la ubicación geográfica.

Comparación entre España y Ecuador:

En España, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (Gobierno de España, 2018) y el Reglamento General de Protección de Datos (Comisión Europea, 2018) son los principales marcos legales que rigen la protección de datos, incluidos los datos manejados por entidades financieras. Estas leyes establecen los principios y requisitos para el procesamiento de datos personales, incluidos los datos financieros, a

continuación, se detallan las características claves:

1. Consentimiento: Las entidades financieras deben obtener el consentimiento informado de los individuos para recopilar y procesar sus datos personales. El consentimiento debe ser libre, específico, informado y otorgado de manera inequívoca.
2. Derechos de los individuos: Los individuos tienen derechos para acceder, rectificar, suprimir y limitar el procesamiento de sus datos personales. También tienen el derecho a la portabilidad de datos y a oponerse al procesamiento en ciertas circunstancias.
3. Medidas de seguridad: Las entidades financieras están obligadas a implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales y prevenir su acceso no autorizado o uso indebido.
4. Transferencias internacionales: La transferencia de datos personales fuera de la Unión Europea está sujeta a restricciones y requerimientos específicos para garantizar un nivel adecuado de protección. (Naciones Unidas, 2022)

Mientras que, en Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPD, 2021) es la ley principal que regula la protección de datos, incluyendo los datos manejados por entidades financieras. Esta ley se inspira en gran medida en los estándares internacionales de protección de datos.

Características clave:

1. Consentimiento: Al igual que en España, las entidades financieras en Ecuador deben obtener el consentimiento de los individuos para el tratamiento de sus datos personales.

2. Derechos de los individuos: Los titulares de datos en Ecuador tienen derechos similares a los de la Unión Europea, como el derecho de acceso, rectificación, supresión, oposición y portabilidad.

3. Seguridad y confidencialidad: Las entidades financieras deben implementar medidas de seguridad adecuadas para proteger los datos personales y garantizar su confidencialidad.

4. Transferencias internacionales: Las transferencias de datos personales a países extranjeros están sujetas a restricciones y requerimientos específicos (Gobierno del Ecuador, 2021)

El Derecho a la Protección de Datos Personales Reconocido por Diversas Normativas Internacionales, como la Unión Europea

El derecho a la protección de datos personales se ha convertido en un tema de gran relevancia en la era digital, donde la información personal se ha vuelto cada vez más susceptible a ser recopilada, almacenada y utilizada por diversas entidades, en respuesta a esta preocupación, diversas normativas internacionales, como la Unión Europea, han reconocido y establecido marcos legales para proteger este derecho fundamental (Meraz Espinoza, 2018).

El derecho a la protección de datos personales es un derecho fundamental que garantiza a los individuos el control sobre su información personal. Implica que los datos personales de las personas deben ser procesados de manera justa, transparente y segura, y solo deben utilizarse para los fines específicos para los cuales se obtuvieron (Godoy, 2017). Además, este derecho asegura que las personas tengan el derecho de acceder, rectificar y eliminar sus datos personales cuando sea necesario, un claro ejemplo es la declaración de Tim Cook, CEO de Apple quien

manifestó que lo importante no era solicitar a sus clientes que comprometan la privacidad en aras de la seguridad, lo crucial era brindarles lo óptimo en ambas áreas, es decir, salvaguardar la información de un individuo equivale a resguardar a toda la comunidad.

La Unión Europea ha desempeñado un papel destacado en el establecimiento de normativas sólidas en materia de protección de datos. El Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), adoptado en 2016 y aplicable desde 2018, se ha convertido en un hito en la regulación de la protección de datos a nivel mundial. En este sentido, el GDPR establece un marco legal robusto que garantiza la privacidad y seguridad de los datos personales de los ciudadanos europeos (Parlamento Europeo, 2023).

Una de las características más destacadas del GDPR es su enfoque basado en el principio de responsabilidad proactiva. Las organizaciones y empresas que recopilan y procesan datos personales deben implementar medidas técnicas y organizativas adecuadas para garantizar la protección de estos datos. Además, se requiere obtener el consentimiento explícito de los individuos para el procesamiento de sus datos, y deben ser informados de manera clara y comprensible sobre cómo se utilizarán sus datos (oportunidades y desafíos en la protección de datos personales).

El GDPR también establece el derecho de los individuos a ser olvidados, lo que implica que las personas tienen el derecho de solicitar que sus datos personales sean eliminados cuando ya no sean necesarios para los fines para los que fueron recopilados. Asimismo, se fortalecen los derechos de acceso y rectificación de los datos personales, brindando a los individuos un mayor control sobre su información. Además del GDPR, la Unión Europea ha adoptado otras normativas y directivas para fortalecer la protección de datos personales. Por ejemplo, la Directiva sobre Privacidad y Comunicaciones Electrónicas establece reglas más estrictas sobre el

uso de cookies y la privacidad en línea. (Parlamento Europeo, 2023).

El derecho a la protección de datos personales es fundamental en la sociedad digital actual. La Unión Europea ha desempeñado un papel destacado en la protección de este derecho a través de normativas sólidas, como el GDPR. Estas normativas garantizan que los datos personales de los individuos sean procesados de manera justa, transparente y segura, y otorgan a los individuos un mayor control sobre su información (Parlamento Europeo, 2023).

La protección de datos personales no solo beneficia a los individuos, sino también a las organizaciones y empresas, ya que fomenta la confianza y la transparencia en el tratamiento de la información personal. Es importante que otros países y regiones tomen ejemplo de las normativas de la Unión Europea y adopten medidas similares para salvaguardar este derecho fundamental en el entorno digital global. Es decir que el derecho a la protección de datos personales es esencial en la sociedad actual y las normativas internacionales, como el GDPR de la Unión Europea, desempeñan un papel crucial en su protección. Garantizar la privacidad y seguridad de los datos personales es fundamental para salvaguardar los derechos individuales y fomentar un entorno digital confiable y ético (Ley 25.326).

Capítulo III: Análisis jurisprudencial y/0 resultados de la investigación

Los Instrumentos Jurídicos para la Protección de Datos Personales en el Ecuador

La protección de datos personales es un tema de vital importancia en la era digital en la que vivimos. Con el avance de las tecnologías de la información y la comunicación, cada vez es más común la recolección, almacenamiento y uso de datos personales por parte de entidades públicas y privadas. En Ecuador, se han implementado diversos instrumentos jurídicos para salvaguardar la privacidad y garantizar el ejercicio de los derechos fundamentales de las personas en relación con sus datos personales (Álvarez, 2017). En este trabajo de titulación, exploraremos los principales instrumentos jurídicos que brindan protección en materia de datos personales en Ecuador, haciendo especial énfasis en la jurisprudencia más relevante en esta materia.

Constitución de la República del Ecuador: La Constitución de la República del Ecuador, promulgada en 2008, es la norma suprema que reconoce y garantiza el derecho a la privacidad y a la protección de los datos personales de los ciudadanos ecuatorianos. En su artículo 66 numeral 19, establece que "las personas tienen derecho al acceso seguro a la información que reposa en archivos, registros y bancos de datos públicos o privados" y que su recolección, almacenamiento, uso y circulación deben ser regulados por la ley. Esta disposición sienta las bases constitucionales para la protección de datos personales en el país.

Ley Orgánica de Protección de Datos Personales (LOPD): La LOPD, aprobada en 2018, constituye la principal normativa en materia de protección de datos personales en Ecuador. Esta ley establece los principios y derechos fundamentales en relación con el tratamiento de datos personales, así como las obligaciones de los responsables y encargados de datos. La LOPD establece los mecanismos para el consentimiento informado, el ejercicio de derechos ARCO

(acceso, rectificación, cancelación y oposición), la transferencia internacional de datos, la notificación de brechas de seguridad, entre otros aspectos relevantes. (Noticias Jurídicas, 2018)

Además, esta ley establece el procedimiento de control estatal para la protección de datos personales por parte de todas las entidades que los traten, mismo que se ha establecido a través de un régimen sancionatorio con medidas correctivas e infracciones (Ley Orgánica de Protección de Datos, 2021, Art. 66). Se dispone por ley que, en caso de incumplimiento de las disposiciones, la Autoridad de Protección de Datos (la futura Superintendencia de Protección de Datos) podrá dictaminar medidas correctivas que pueden consistir, entre otras en:

A) El cese del tratamiento, bajo determinadas condiciones o plazos;
B) La eliminación de los datos; y,
C) La imposición de medidas técnicas, jurídicas, organizativas o administrativas a garantizar un tratamiento adecuado de datos personales.

Las medidas indicadas podrán ser establecidas previo informe de la unidad técnica competente, y siguiendo las reglas establecidas para ello en el artículo 66 de la Ley. En los siguientes artículos de se establecen infracciones tanto leves como graves para el responsable del tratamiento de los datos como para el encargado del tratamiento de datos, en función del incumplimiento de la ley y de las funciones que para ellos se encuentran estipuladas. A partir del artículo 71 de la LOPD se establecen las sanciones correspondientes para las infracciones leves y en el artículo 72 las de las infracciones graves, marcando diferencias para los responsables de entidades públicas y privadas, pues mientras que a los servidores públicos responsables se les determina multas que van de uno a veinte salarios básicos unificados, a los responsables que sean entidades privadas se aplicará una multa de entre el 0.1% y el 1% calculada sobre el volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la

imposición de la multa, todo lo anterior dependiendo de la gravedad de la infracción. Para la aplicación del principio de proporcionalidad al determinar la multa se deberán tener en cuenta presupuesto como: la intencionalidad, la reiteración, la naturaleza del perjuicio, la reincidencia.

El procedimiento administrativo de control de protección de datos de carácter personal se establece por medio de un régimen sancionatorio con medidas correctivas e identificación de infracciones que se establecen a partir del capítulo XI de la LOPD, teniendo en cuenta que el artículo 76 de la LOPD establece que será la Autoridad de Protección de Datos Personales el órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales, y de llevar a cabo la supervisión de la protección de derechos y las sanciones que se requieran. Como se mencionó anteriormente, la aplicación de las medidas correctivas que surjan del procedimiento de control se encuentra establecidas por el artículo 66 de la LOPD, y en él se determina un procedimiento de control para las infracciones que son leves, graves y muy graves.

Al ser la aplicación de medidas correctivas objeto de materia administrativa, su régimen de procedimiento debe ser conducido por el Código Orgánico Administrativo, en tanto las sanciones comprenden un procedimiento administrativo sancionador. Concretamente, el artículo 66 determina que para el presunto cometimiento de una infracción leve, la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio, haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida; mientras que para el presunto cometimiento de una infracción grave, la Autoridad de Protección de Datos Personales aplicará en primera instancia medidas correctivas. Si las medidas correctivas fueren cumplidas de forma tardía, parcial o defectuosa, la Autoridad de Protección de Datos Personales, aplicará las

sanciones que corresponden a las infracciones graves, activando para el efecto el procedimiento administrativo sancionatorio y haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida; y, cuando se esté frente el presunto cometimiento de una infracción muy grave, la Ley Orgánica de Protección de Datos (2011) menciona en el artículo 46 que la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida. Lo anterior lo corrobora lo establecido en el Reglamento a la Ley Orgánica de Protección de Datos Personales, ya que en su artículo 90 determina que "en los casos en que se presuma el cometimiento de alguna de las infracciones previstas en la Ley, la Autoridad de Protección de Datos iniciará el correspondiente procedimiento administrativo sancionatorio, de conformidad con las disposiciones establecidas en el Código Orgánico Administrativo" (Ley Orgánica de Protección de Datos Personales, 2011, Art. 90).

Para que el control mencionado en el párrafo anterior sea efectivo primero debe de crearse la Superintendencia de Protección de Datos Personales, misma que hasta el momento de terminar este trabajo, no ha sido aun creada, pues a pesar de que por parte del poder ejecutivo ha sido remitida en más de una ocasión una terna para la elección del Consejo de Participación Ciudadana y Control Social del Superintendente de Protección de Datos Personales, ese poder estatal no se ha dado a la tarea de realizar la elección para que consecuentemente se cree el organismo de protección de datos (Redacción Expreso, 2023).

En relación con el Código Orgánico Administrativo y la protección de datos personales este menciona en el artículo 24 que existe el "principio de protección de la intimidad", es decir, que cuando las entidades gubernamentales manejen información personal, estas tienen la

obligación de respetar y asegurar el derecho a la intimidad personal y familiar, así como a preservar la vida privada de las personas, sin embargo se limita únicamente a instituciones públicas (Código Orgánico Administrativo, 2017, Art. 24).

Sin embargo, plantea un esquema detallado de como el procedimiento administrativo interviene para que se dé una sanción, el cual inicia con la petición del interesado que posteriormente tiene un plazo de 10 días para la subsanación, que en el caso de no existir procede a la emisión de una resolución de desistimiento (Código Orgánico Administrativo, 2017, Art. 140). Posteriormente, tiene lugar la orden de procedimiento para iniciar el trámite, que fija el termino de prueba y prosigue con la notificación del acto administrativo, que puede llevar a la ejecución o a la terminación del procedimiento, que tiene como causales según el Artículo 201 del COA los siguiente: "el silencio administrativo, el desistimiento, el abandono, la caducidad del procedimiento o de la potestad pública, la imposibilidad material de continuarlo por causas imprevistas, y la terminación convencional" (Código Orgánico Administrativo, 2017, Art. 201).

Posterior a esto, y en un plazo no mayor a 50 días puede tener lugar el recurso de apelación que tiene una fecha máxima de un mes para el recurso de apelación, que puede suspender la ejecución. Finalmente, el recurso extraordinario de revisión se puede admitir en máximo 20 días y resolver en un mes, tal como se menciona en el artículo correspondiente a "impugnación" (Código Orgánico Administrativo, 2017, Art. 217).

En relación con el procedimiento administrativo sancionador, este se rige por el principio de caducidad de la potestad sancionadora, según el cual la administración pública debe concluir el procedimiento en el plazo establecido por el código correspondiente tal como lo menciona en el artículo 244 donde establece que "la potestad sancionadora caduca cuando la administración

pública no ha concluido el procedimiento administrativo" (Código Orgánico Administrativo, 2017, Art. 244), es decir, que en caso de caducidad, el órgano competente emitirá una certificación, a solicitud del inculpado, indicando la caducidad de la potestad y el archivo de las actuaciones. Así mismo, es importante destacar que la prescripción del ejercicio de la potestad sancionadora varía según la gravedad de la infracción, con plazos de uno, tres y cinco años para infracciones leves, graves y muy graves, respectivamente.

La prescripción de las sanciones sigue el mismo plazo de caducidad de la potestad sancionadora, considerándose cuando no ha habido resolución. Además, se establece un plazo específico para la prescripción cuando el acto administrativo ha causado estado, siendo este plazo contado desde el día siguiente a dicho estado. El artículo 245 del Código Orgánico Administrativo (2017) menciona lo siguiente:

> El ejercicio de la potestad sancionadora prescribe en los siguientes plazos:
>
> A) Al año para las infracciones leves y las sanciones que por ellas se impongan
>
> B) A los tres años para las infracciones graves y las sanciones que por ellas se impongan
>
> C) A los cinco años para las infracciones muy graves y las sanciones que por ellas se impongan (Código Orgánico Administrativo, 2017, Art. 245).

El procedimiento sancionador inicia de oficio por acuerdo del órgano competente, notificando a la parte denunciante y a la persona inculpada y se destaca la posibilidad de reconocimiento de responsabilidad y pago voluntario, así como la comunicación de indicios de infracción durante cualquier fase del procedimiento. Para esto, el artículo 248 del Código Orgánico Administrativo (2017) establece:

> 1. En los procedimientos sancionadores se dispondrá la debida separación entre la función instructora y la sancionadora,

> 2. En ningún caso se impondrá una sanción sin que se haya tramitado el necesario procedimiento.
>
> 3. El presunto responsable por ser notificado de los hechos que se le imputen, de las infracciones que tales hechos puedan constituir y de las sanciones que, en su caso, se le pueda imponer, así como de la identidad del instructor, de la autoridad competente para imponer la sanción y de la norma que atribuya tal competencia.
>
> 4. Toda persona mantiene su estatus jurídico de inocencia y debe ser tratada como tal, mientras no exista un acto administrativo firme que resuelva lo contrario (Código Orgánico Administrativo, 2017, Art. 248).

Las garantías del procedimiento incluyen la debida separación entre la función instructora y sancionadora, el derecho a ser notificado de los hechos imputados, y la presunción de inocencia hasta que exista un acto administrativo firme en contrario, por lo cual el procedimiento se inicia mediante un acto administrativo de inicio que identifica a la persona responsable, los hechos imputados y la norma que atribuye competencia. Durante el procedimiento, se pueden practicar pruebas necesarias para la determinación de los hechos y la responsabilidad.

El dictamen del órgano instructor contiene la determinación de la infracción, elementos de la instrucción y la sanción propuesta, es así como la resolución final incluye la determinación de la persona responsable, la infracción cometida, la valoración de la prueba, la sanción impuesta o la declaración de inexistencia de infracción, y las medidas cautelares necesarias. Se prohíbe la concurrencia de sanciones administrativas cuando exista identidad de sujeto, objeto y causa, y en caso de infracción penal, el expediente se remite a la autoridad competente.

Habeas Data: El habeas data es un concepto jurídico que se refiere al derecho que tiene una persona de controlar la información que concierne a su propia persona, especialmente en lo

que respecta a datos personales. Este derecho permite a los individuos conocer, acceder, rectificar y, en algunos casos, suprimir la información que se encuentra almacenada sobre ellos en bases de datos y registros (Godoy, 2017).

El alcance de este concepto no se limita únicamente a la recolección y almacenamiento de datos, sino también su tratamiento, uso y divulgación. Zamora (2010) menciona que incluye información como datos personales básicos, historiales médicos, antecedentes financieros, y cualquier otra información que pueda identificar de manera directa o indirecta a una persona. El contenido del habeas data busca proteger la privacidad y autonomía de los individuos, otorgándoles el control sobre su información personal.

En la actualidad, la figura del Habeas Data en el Ecuador se encuentra normada en el artículo 92 de la Constitución del Ecuador, donde se establece la "Acción de hábeas data". Esta disposición garantiza a toda persona, ya sea en ejercicio de sus propios derechos o en calidad de representante legitimado, el derecho de conocer la existencia y acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que se encuentren en entidades públicas o privadas, ya sea en formato físico o electrónico. Asimismo, se le concede el derecho de conocer el uso que se le da a esta información, su propósito, el origen y tipo de datos personales, así como el periodo de validez del archivo o banco de datos (Constitución del Ecuador, 2008, Art. 92).

En el marco de esta regulación, se establece que las personas responsables de estos bancos o archivos de datos personales tienen la facultad de difundir la información archivada únicamente con la autorización expresa del titular de los datos o cuando así lo disponga la ley. Es fundamental destacar que la persona titular de los datos goza del derecho de solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su

rectificación, eliminación o anulación.

En situaciones que involucren datos sensibles, cuyo archivo debe contar con la autorización expresa de la ley o del titular de la información, se impone la obligación de adoptar las medidas de seguridad necesarias para salvaguardar la confidencialidad y proteger la integridad de dichos datos. De esta manera, la regulación busca garantizar no solo el acceso a la información personal, sino también la preservación de la privacidad y seguridad de los datos sensibles, fortaleciendo así los derechos fundamentales de los individuos en el ámbito de la protección de datos en Ecuador (Arce, 2009).

Finalmente, el habeas data y la protección de datos están intrínsecamente relacionados, ya que ambos se centran en salvaguardar la privacidad y el control que las personas tienen sobre su información personal. La protección de datos, como concepto más amplio, engloba medidas y regulaciones que buscan garantizar el uso ético y legal de la información personal, mientras que el habeas data se concentra en el derecho específico de los individuos a ejercer control sobre sus datos. En la era digital, donde la recopilación y el procesamiento de datos son omnipresentes, el habeas data adquiere una importancia crucial. La creciente interconexión y la digitalización de la información exigen una protección robusta de los derechos individuales, y el habeas data se erige como un mecanismo esencial para empoderar a las personas en el control y gestión de su propia información en el entorno digital.

Jurisprudencia relevante: A lo largo de los años, los tribunales ecuatorianos han emitido fallos que han contribuido a consolidar la protección de datos personales como un derecho fundamental. Destacan algunos casos emblemáticos, como la sentencia No. 55-14-JP de la Corte Constitucional que declaró la inconstitucionalidad de una disposición que permitía la retención de datos de comunicaciones electrónicas sin orden judicial, y la sentencia T-277/15 de

la Corte Constitucional Colombiana que estableció el derecho al olvido en casos específicos (Plúa, 2017). Otra sentencia importante es la 025-15-SEPCC que establece las dimensiones utilitarias del Habeas Data, como lo son: Habeas data informativo (derecho de acceso), Habeas data aditivo (derecho de rectificación o modificación), Habeas data correctivo (derecho de corrección), habeas data de reserva (derecho de confidencialidad), Habeas data cancelatorio (derecho de exclusión de información sensible), mismos que corresponden a los conocidos como derechos ARCO en materia de protección de datos como lo son el derecho de Acceso, establecido en el artículo 13 de la LOPD que establece que " El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales"; El derecho de rectificación que en el artículo 14 de la Ley establece que "El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos"; el derecho de cancelación o eliminación, el cual se establece en el artículo 15 de la LOPD y manda que "El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales"; mientras que el derecho de oposición se establece en el artículo 16 de la misma ley e indica que "El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales". Estas decisiones judiciales han sentado importantes precedentes en la protección de datos personales en Ecuador, y han contribuido a la interpretación y aplicación de la legislación vigente, teniendo en cuenta que la LOPD es nueva, esa sentencia explica adecuadamente el alcance de los derechos de protección de datos que fueron luego recogidos en la Ley.

Sentencia No. 2064-14-EP/21

El fallo No. 2064-14-EP/21 (Corte Constitucional del Ecuador, 2021) marca un hito en la

protección de datos personales ya que la corte procura definir adecuadamente términos necesarios para proteger los datos personales, como son el concepto de datos, de tratamiento de datos en la esfera personal y doméstica y consentimiento del titular, sentando las bases de los conceptos contenidos actualmente en la Ley Orgánica de Protección de Datos Personales y utilizando la conceptualización que sobre estos términos había ya realizado el Tribunal Europeo de Derechos Humanos y el Reglamento Europeo de Protección de Datos Personales. Esta sentencia determino:

> En el caso concreto, las fotografías íntimas de la actora constituyen datos personales; por lo que, la parte accionada, al realizar un tratamiento de estos datos sin su consentimiento, vulneró los derechos a la protección de datos personales o autodeterminación informativa, imagen, honra, buen nombre e intimidad (Corte Constitucional del Ecuador, 2021).

Un elemento interesante de esta sentencia es que se refiere a la protección de datos por medio de la acción constitucional de Habeas Data, : lo cual ha sido determinante, debido que si bien es cierto, no se encontraba en ese momento una Ley que regulase la protección de los datos, si existía una forma de proteger los datos como constitucionalmente se reconoce en el artículo 66 numeral 19 de la constitución. Empero del reconocimiento de lo anterior, no es ajeno el que los hechos por los que se da la sentencia de la Corte Constitucional tuvieron lugar en 2014 y recién en el año 2021 se emitió la sentencia por parte de la Corte. Esto representa un cambio significativo en la legislación ecuatoriana y confirma que la acción de hábeas data es efectiva para resguardar derechos individuales como lo son el derecho a la intimidad, honor y buen nombre, y protección de datos personales, ligados a la integridad de cada persona. Por consiguiente, en casos de menoscabo de la honorabilidad y dignidad, la parte afectada podría

tener derecho a una reparación integral debido al perjuicio sufrido por el tratamiento de sus datos personales. Si bien en Ecuador a la fecha de la sentencia no existía un ordenamiento que especifique con claridad lo que es un dato personal y lo que conlleva el uso y tratamiento, la corte se basó en reglamentos como el de la Unión Europea mismo que es un modelo para seguir para otras legislaciones, además de que en Ecuador existía ya un acuerdo ministerial emitido por el Ministerio de Telecomunicaciones que iba en concordancia con lo plasmado por el Reglamento Europeo de Protección de Datos Personales.

La Corte Constitucional de la República del Ecuador, en el caso No. 2064-14-EP/21 (Corte Constitucional del Ecuador, 2021), subraya que el término "datos personales" y la información relacionada con una persona deben interpretarse de manera extensa, abarcando cualquier información que aluda directa o indirectamente a cualquier aspecto de una persona o sus posesiones, en sus diferentes ámbitos o dimensiones, y que puede ser exigida a través de la garantía de hábeas data. Se determinó que el hábeas data procede ante un uso no autorizado de los datos personales que atenta contra el derecho a la protección de datos de carácter personal, además se destacó la importancia de la protección de datos personales como herramienta fundamental para garantizar los derechos humanos y la privacidad de las personas. Además, se estableció que el habeas data era la vía adecuada para proteger los derechos de la persona afectada. En este sentido, la Corte estableció que existe un derecho fundamental que tiene toda persona a conocer, actualizar y rectificar la información que se tenga sobre ella en bancos de datos y archivos de entidades públicas y privadas.

En este sentido, la corte analiza los siguientes puntos respecto de la aplicación de esta garantía: ¿Cuál es el alcance del concepto de dato personal en nuestro ordenamiento jurídico?; ¿Qué debe entenderse por uso/tratamiento de datos personales?; Delimitación del tratamiento

de datos en la esfera exclusivamente personal o doméstica y sus efectos; Alcance del concepto del "consentimiento" del titular de datos personales en el tratamiento por parte de un tercero; La procedencia de la acción de hábeas data cuando existen elementos en el caso inherentes a la justicia ordinaria, entre otras.

A pesar de que, en la apelación del habeas data, la Corte Provincial en segunda instancia, determinó que no hubo vulneración alguna y que no daba a lugar a la acción presentada, puesto que la actora en su momento de enviar la documentación con sus datos personales, esta lo hizo de manera consciente y voluntaria, y no tomaron en cuenta la malversación y el uso indebido de dichas fotos que contenían datos personales, sin embargo, la corte constitucional resolvió el caso.

La Corte Constitucional del Ecuador se pronunció de esta manera: "datos personales e información sobre una persona", tal como se encuentran recogidos en nuestra Constitución y en función de una interpretación conforme al principio pro homine, deben ser entendidos en su forma más amplia, en el sentido de toda información que haga referencia de forma directa o indirecta a cualquier aspecto relativo a una persona o sus bienes, en sus distintas esferas o dimensiones; susceptible de ser exigida a través de la garantía de hábeas data. Así se advierte que basta que la información –más allá de la forma en que esté contenida– incluya o comunique un aspecto de la persona –objetivo o subjetivo–; o guarde relación con ella, en función de su contenido, finalidad o resultado, para ser considerada como "dato personal" y tomó en cuenta la definición de dato personal para la unión europea: Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica,

genética, psíquica, económica, cultural o social de dicha persona.

Luego dieron a conocer a que se refiere con el tratamiento de datos personales donde determinaron que el tratamiento de datos personales se refiere a una operación técnica que implica diversas acciones relacionadas con la información personal. Aunque su definición puede variar en diferentes jurisdicciones y evolucionar debido a avances tecnológicos, en nuestro sistema legal, se define como la obtención, registro, organización, conservación, modificación, consulta, uso, transmisión, difusión y otras acciones que permiten el acceso, comparación o eliminación de datos personales.

El consentimiento de la persona que proporciona sus datos fue previsto como un aspecto crucial, especialmente en situaciones donde se pueden enfrentar derechos constitucionales, como la libertad de expresión o el interés público, al publicar información sobre una persona. El juez debe ponderar estos derechos en función de las circunstancias del caso, determinando cuál prevalece y en qué medida, según las posibilidades legales y factuales. Es importante notar que el nivel de privacidad varía entre figuras públicas y personas no públicas. En principio, cualquier tratamiento de datos personales debe contar con el consentimiento explícito y claro del titular, a menos que la ley lo permita, con ciertas excepciones detalladas en párrafos anteriores. Esto significa que se deben cumplir ciertos elementos para que se considere que el consentimiento es válido.

Surgió la incógnita si el tratamiento realizado de los datos personales de la actora vulnera los derechos invocados por ella en su demanda de hábeas data, esto es, a la protección de datos personales y a la autodeterminación informativa, imagen, honra y buen nombre, e intimidad.

Donde los jueces entablaron como punto de partida principal la constitución del Ecuador donde queda establecido que es un derecho en su artículo 66 numeral 19, al igual que hacen

mención en el artículo 92 del mismo texto.

En cuanto a las medidas tomadas para proteger los derechos de la persona afectada, la Corte Constitucional del Ecuador ordenó la eliminación de la información personal y sensible publicada en el medio de comunicación, así como la adopción de medidas para evitar que se vuelva a vulnerar los derechos de la persona afectada. Esta medida es importante porque demuestra que la Corte está comprometida con la protección de los derechos humanos y la privacidad de las personas.

Por último, la sentencia demuestra la necesidad de que existan mecanismos efectivos de protección de datos personales en el Ecuador. La regulación en esta materia es casi nula y la jurisprudencia ecuatoriana ha desarrollado poco este derecho fundamental.

A pesar de que el fallo se emitió en 2021, reflejando un cambio significativo en la legislación, el caso ocurrió en 2014, resaltando la eficacia de la acción de hábeas data. La Corte estableció que existe un derecho fundamental a conocer, actualizar y rectificar la información en bancos de datos, y aunque la corte se basó en regulaciones europeas y acuerdos ministeriales, se resalta la falta de regulación específica en Ecuador en ese momento.

En este contexto, la sentencia aborda diversos aspectos del tratamiento de datos, incluyendo el alcance del consentimiento y las medidas para proteger a la persona afectada, conceptos claves que dieron lugar posteriormente a la Ley Orgánica de Protección de Datos a nivel nacional, así mismo, posterior al fallo de la Corte Constitucional ordenó la eliminación de información sensible y la adopción de medidas preventivas. Finalmente, la sentencia destaca la necesidad de mecanismos efectivos de protección de datos en Ecuador y plantea la importancia de analizar la protección de datos en el ámbito financiero, combinando los conceptos de la sentencia con la responsabilidad de las instituciones financieras en el manejo de datos.

Normativas complementarias: Además de la LOPD, existen otras normativas que complementan el marco legal de protección de datos en Ecuador. Entre ellas, se encuentran las normas sectoriales específicas que regulan el tratamiento de datos en áreas como el sector financiero como es la Ley de Protección y Defensa al usuario de Servicios Financieros, y el Esquema Gubernamental de Seguridad de la Información en aquellos datos que maneja el Ministerio de Salud Pública, entre otros. Estas normativas se orientan a garantizar una protección integral y específica de los datos personales en sectores sensibles. La existencia de estas normas complementarias demuestra el compromiso del Estado ecuatoriano en abordar la protección de datos personales desde una perspectiva sectorial y especializada.

La Superintendencia de Bancos (2022) en su documento titulado Ley de Protección y Defensa al Usuario de Servicios Financieros menciona en su sección 3 “Derechos del Usuario del Sistema Financiero” que los usuarios tienen el derecho de conocer y acceder a la información que las entidades financieras poseen sobre ellos, así como conocer la fuente de dicha información y exigir la rectificación de datos inexactos. Además, tienen el derecho a que su información personal sea tratada de acuerdo con ciertos principios, incluyendo la autorización previa y expresa para la recopilación de datos, la posibilidad de revocar dicha autorización, y la garantía de que sus datos sean tratados con apego a los principios y leyes establecidas. También tienen derecho a que sus datos sean precisos, conservados por un tiempo determinado, y accesibles de manera gratuita, así como a recibirlos en un formato actualizado y estructurado, sin olvidar que cuentan con el derecho de recibir protección y de demandar medidas efectivas para garantizar la seguridad de sus operaciones financieras ante la Superintendencia de Bancos u otras instancias pertinentes.

Así mismo, la protección de datos personales en Ecuador se encuentra respaldada por un

sólido marco normativo, encabezado por la Constitución y la Ley Orgánica de Protección de Datos Personales. La jurisprudencia ecuatoriana ha jugado un papel fundamental en la consolidación de este derecho fundamental, sentando importantes precedentes en la materia. No obstante, es necesario continuar fortaleciendo y actualizando el marco legal en respuesta a los desafíos y avances tecnológicos que surgen constantemente, garantizando así la protección efectiva de los datos personales y la privacidad de los ciudadanos ecuatorianos en un entorno digital en constante evolución. La protección de datos personales es un derecho fundamental que debe ser protegido y promovido en beneficio de la sociedad en su conjunto (Russel, 2023).

La Agencia Española de Protección de Datos impuso una multa de 70.000 euros a CaixaBank Payments & Consumer, una filial completamente propiedad de CaixaBank, por el tratamiento no autorizado de los datos personales de un usuario. Esta sanción se basa en una denuncia presentada por un cliente de la entidad financiera, quien afirmó que, a pesar de que se había dictado una sentencia judicial en mayo de 2019 anulando una deuda asociada a una tarjeta de crédito 'Visa Classic Club Ahora', CaixaBank y empresas de recobro continuaron reclamándole el pago.

La sentencia judicial establecía que el cliente solo estaba obligado a devolver la cantidad prestada, sin incluir intereses ni gastos adicionales. El reclamante cumplió con esta orden en septiembre de 2020, ingresando la cantidad prestada más los intereses legales en la cuenta del juzgado. En noviembre de 2020, el juzgado notificó a CaixaBank Payments & Consumer que el pago había sido realizado por el usuario. El cliente proporcionó una carta del Grupo CaixaBank, fechada el 24 de diciembre de 2020, en la cual se confirmaba la nulidad del contrato y se daban instrucciones para cesar las reclamaciones de impago. Sin embargo, el cliente afirma que el 23 de julio de 2021 recibió un mensaje de texto (SMS) de una empresa de recobro en nombre de

CaixaBank Payments & Consumer, exigiendo el pago de la deuda. La entidad está evaluando la posibilidad de recurrir esta sanción ante la Audiencia Nacional.

Caso Santander

La Corte de Apelaciones de Santiago confirmó la sentencia del Quinto Juzgado Civil de Santiago que condenó al Banco Santander por negligencia en el manejo de datos personales de sus clientes. El caso se originó cuando se descubrió que el banco había arrojado documentación bancaria de sus clientes en un vertedero ilegal en octubre de 2015. La sentencia del tribunal de alzada respalda la conclusión del juzgado de primera instancia, que estableció que el banco no había tomado las medidas adecuadas para proteger los datos de sus clientes, lo cual contraviene la Ley de Protección de Datos. La ley establece una serie de obligaciones para el responsable de las bases de datos, que incluyen el respeto de los derechos fundamentales de los titulares de datos, el cuidado diligente de los datos, la eliminación o cancelación de los datos personales cuando sea necesario y el uso de los datos para los fines para los cuales se recopilaron. En este caso, el abandono de documentos que contenían datos personales en un lugar público fue considerado una infracción a la obligación general de resguardar la seguridad de los datos y vulneró el derecho a la privacidad de los titulares. Además, se consideró una violación a la obligación específica de utilizar los datos para los fines para los cuales se recopilaron y de eliminarlos cuando ya no eran necesarios (Santander, 2023).

El fallo fue dividido, y uno de los jueces disidentes estuvo a favor de otorgar una indemnización por daño moral a los demandantes. Sin embargo, la sentencia en alzada rechazó dicha indemnización, argumentando que el testimonio de los testigos presentados por los demandantes era genérico y no acreditaba un daño moral específico. En resumen, el caso involucra una condena al Banco Santander por infringir la protección de datos de sus clientes al

abandonar documentos en un lugar público, lo cual violó las obligaciones legales de resguardo y uso adecuado de los datos personales (Diario Constitucional, 2018).

En los dos casos mencionados, tanto la multa impuesta a CAIXABANK PAYMENTS & CONSUMER EFC, EP, S.A.U. como la condena al Banco Santander, están relacionados con infracciones en materia de protección de datos personales. Ambas entidades financieras enfrentaron consecuencias legales por no cumplir con las normativas establecidas para salvaguardar la privacidad y seguridad de la información de sus clientes (EuropaPress, 2023).

En el caso de CAIXABANK PAYMENTS & CONSUMER EFC, EP, S.A.U., la Agencia Española de Protección de Datos impuso una multa de 6 millones de euros por diversas infracciones, como el tratamiento ilícito de datos personales, la falta de base legal para el tratamiento de datos y la falta de transparencia en la recopilación de datos. Estas infracciones se produjeron en el contexto de la contratación de productos financieros por teléfono, donde se recopilaban datos personales sin el consentimiento adecuado de los usuarios (EuropaPress, 2023).

Por otro lado, el Banco Santander fue condenado por la Corte de Apelaciones de Santiago por negligencia en el manejo de datos personales de sus clientes. El banco arrojó documentos bancarios en un vertedero ilegal, lo que constituyó una infracción a la Ley de Protección de Datos en Chile. Se determinó que el banco no había tomado las medidas adecuadas para proteger los datos de sus clientes y había incumplido con sus obligaciones de resguardo y uso adecuado de los datos.

En términos de similitudes, ambos casos involucran la vulneración de normativas de protección de datos personales, lo que resultó en sanciones y condenas legales. En ambos casos, las entidades financieras no cumplieron con sus responsabilidades de resguardar la privacidad y seguridad de la información de sus clientes, lo que puso en riesgo la confidencialidad de los

datos personales. Sin embargo, también existen diferencias significativas entre los casos. En el caso de CAIXABANK PAYMENTS & CONSUMER EFC, EP, S.A.U., se trata de una multa impuesta por la Agencia Española de Protección de Datos, mientras en el caso del Banco Santander, se trata de una condena por parte de un tribunal chileno. Además, las infracciones específicas difieren en cada caso: el primero se centra en el tratamiento ilícito de datos y la falta de transparencia, mientras que el segundo se relaciona con el abandono negligente de documentos bancarios.

Ambos casos destacan la importancia de cumplir con las normativas de protección de datos y resguardar la privacidad de los clientes. La imposición de multas y condenas en casos

como estos envía un mensaje claro de que las instituciones financieras deben garantizar la adecuada gestión y protección de los datos personales que manejan.

Jurisprudencia sobre protección de datos personales y sus implicaciones en las instituciones financieras

En el ámbito financiero, la protección de datos personales ha adquirido una relevancia cada vez mayor en los últimos años. Con el avance de la tecnología y la digitalización de los servicios financieros, se ha generado una enorme cantidad de información personal sensible que requiere de una adecuada protección y salvaguardia. La jurisprudencia ha jugado un papel fundamental en el desarrollo de las normas y principios que rigen la protección de datos en el ámbito financiero, y en este trabajo se investiga las implicaciones que tiene para las instituciones financieras ecuatorianas.

La jurisprudencia en la protección de datos personales en el ámbito financiero ha sido marcada por la necesidad de equilibrar los intereses de las instituciones financieras en el procesamiento de datos para la prestación de servicios, con el respeto a los derechos fundamentales de privacidad y protección de datos de los titulares de dicha información. En sus primeras etapas, la jurisprudencia se centró en establecer los principios básicos para el tratamiento de datos personales, como el consentimiento informado, la finalidad y la minimización de datos (Suprema Corte de Justicia de la Nación, 2018).

Con el tiempo, la jurisprudencia ha evolucionado hacia la creación de estándares más estrictos en términos de seguridad y confidencialidad de los datos personales en el ámbito financiero. Se han establecido criterios más claros sobre la responsabilidad de las instituciones financieras en la protección de los datos de sus clientes, así como la obligación de informar adecuadamente sobre el tratamiento de datos y los derechos de los titulares. Además, se han

establecido sanciones más severas para aquellos que no cumplan con las normas de protección de datos (Suprema Corte de Justicia de la Nación, 2018).

La evolución de la jurisprudencia en la protección de datos personales en el ámbito financiero tiene diversas implicaciones para las instituciones financieras ecuatorianas. En primer lugar, implica la necesidad de adoptar medidas de seguridad y protección de datos más robustas. Las instituciones financieras deben garantizar la confidencialidad, integridad y disponibilidad de los datos personales que manejan, implementando políticas y procedimientos de seguridad acordes con los estándares establecidos por la jurisprudencia (Carrillo, 2021).

Además, las instituciones financieras deben asegurarse de obtener el consentimiento informado de los titulares de datos y cumplir con las obligaciones de transparencia en cuanto al tratamiento de datos personales. Esto implica proporcionar información clara y comprensible sobre los fines del tratamiento, los derechos de los titulares y las medidas de seguridad implementadas (Ley Orgánica de Protección de Datos, 2021, Art. 8).

Asimismo, la jurisprudencia ha establecido que las instituciones financieras deben adoptar un enfoque proactivo y demostrar que han implementado mecanismos adecuados de protección de datos. Esto implica la necesidad de realizar evaluaciones de impacto en la protección de datos, mantener registros actualizados de las actividades de tratamiento y llevar a cabo revisiones periódicas para garantizar la exactitud y actualización de los datos (González, 2021).

Estas implicaciones se centran en la necesidad de adoptar medidas más rigurosas de seguridad y protección de datos, garantizar el cumplimiento de las obligaciones de transparencia y obtener el consentimiento informado de los titulares de datos. Además, las instituciones financieras deben adoptar un enfoque proactivo y demostrar la implementación de mecanismos

adecuados de protección de datos. En este contexto, las instituciones financieras ecuatorianas deben estar al tanto de la evolución de la jurisprudencia en materia de protección de datos y adaptarse a los estándares y exigencias establecidos. Esto les permitirá no solo cumplir con la normativa vigente, sino también generar confianza en sus clientes y fortalecer su reputación en un entorno cada vez más digital y orientado a la privacidad.

Banco Pichincha: Recencia al caso institución financiera

Uno de los casos más relevantes en los que ha existido una clara vulneración al derecho de protección de datos personales es el ocurrido el año 2021 con la institución financiera Banco Pichincha, mismo que ha sido elegido en este proyecto de investigación para analizar lo ocurrido por ser el banco más grande del Ecuador. De acuerdo a como lo indica una nota periodística publicada por Barra Espaciadora (2021) entre el 9 y 12 de febrero se tuvo conocimiento a través de redes sociales de que se habían filtrado por parte de un grupo de cibercriminales conocidos como Corp. Horus, indicando a través de sus cuentas que habrían sustraído 80 Gigabytes de datos sensibles pertenecientes a los clientes de la institución financiera entre los que se mencionan como datos de tarjetas de crédito, datos de acceso a intranet y datos que hacen identificable a una persona.

Por otro lado, el Banco Pichincha (2021) emitió un comunicado oficial en el que aseguraban que la noticia de que le habían sido sustraídos datos personales es falsa y aseveraban que sus sistemas no habían sido vulnerados. Sin embargo, los ciberdelincuentes exigían al Banco Pichincha 30 millones de dólares en criptomonedas para evitar que se continúe difundiendo la información, mientras que surgían testimonios de personas que habían podido verificar que sus datos se encontraban en la lista de datos filtrados. Finalmente, el Banco Pichincha se ratificó en

que sus sistemas no habrían sufrido vulneraciones de seguridad, pero sí manifestó que existió un acceso no autorizado al sistema de un proveedor de servicios de mercadeo, y que los datos filtrados en redes sociales correspondían a ese incidente de seguridad, para lo que ya había el banco presentado una denuncia en fiscalía.

Con lo aseverado en el comunicado del banco se puede colegir que fue un intento de deslindarse de responsabilidad sobre la filtración de datos cuyos titulares habían consentido a ser tratados por parte del Banco Pichincha. Finalmente, a pesar de que para aquel momento ya existía y estaba vigente la Ley Orgánica de Protección de Datos Personales, al no existir la Superintendencia de Protección de Datos Personales, no hubo una entidad que pudiera verificar la responsabilidad del Banco y con ello determinar una multa económica que sirva de detrimento contra la ligereza con la que se vio que se tomó el asunto por parte del banco, especialmente, teniendo en cuenta que no fue el único incidente contra los sistemas de seguridad de la entidad bancaria de ese año.

De este caso se resalta la importancia de una entidad supervisora respecto de la protección de datos personales, siendo que no ha existido aún hoy una determinación de responsabilidad frente a la filtración ocurrida. El hecho de que la filtración no se haya dado por cuenta de afectación a los sistemas de la entidad financiera, no equivale a que no sea responsable, teniendo en cuenta que no los titulares de los datos consintieron en el tratamiento de sus datos por parte de la entidad bancaria, y habría que realizar una revisión contractual para verificar si también existió un consentimiento para que sean tratados por la compañía de mercadeo de quien se alega fueron vulnerados sus sistemas. En caso de haber existido una transferencia de datos por parte del banco a la compañía de mercadeo, debía existir consentimiento por parte del titular de los datos, sino se estaría frente a una clara infracción de lo

determinado en la Ley de Protección de Datos Personales. Como tal, la responsabilidad no solo recaería sobre quien no haya tomado las medidas adecuadas para la protección de los datos personales, que en este caso se indica fue una compañía de mercadeo, sino también para quien haya entregado o transferido datos personales del titular sin su consentimiento, mismo que debe ser informado, es decir que el titular debe conocer toda la información referente al tratamiento de sus datos.

Conclusiones

En conclusión, en la sociedad contemporánea la interconexión entre los avances tecnológicos y la digitalización de la información ha transformado radicalmente la forma en que vivimos y nos relacionamos. La revolución digital ha catapultado el uso de nuevas tecnologías por lo cual esta creciente dependencia de la tecnología ha elevado la importancia de la protección de datos, dado que la recopilación masiva, procesamiento y almacenamiento de información personal plantean desafíos significativos en términos de privacidad y seguridad. En este contexto, se evidencia la necesidad de una regulación robusta y actualizada que salvaguarde los derechos fundamentales de las personas en la era digital, reconociendo la compleja interacción entre la tecnología y la información en nuestra sociedad contemporánea.

Por eso, la protección de datos personales, consagrada como un derecho fundamental, engloba una red interconectada de derechos que emergen de su núcleo. La legislación, como la Ley Orgánica de Protección de Datos Personales, reconoce la información como un bien jurídico tutelado, identificando datos como nombre, dirección, correo electrónico, entre otros, donde el derecho a la protección de datos, entendido como el derecho a la autodeterminación informativa, a la intimidad y a la privacidad, se configura como un derecho fundamental autónomo. El Tribunal Constitucional Español distingue sus facultades específicas, permitiendo al titular controlar y exigir acciones concretas sobre sus datos y de esta manera, se confirma que la protección de datos personales no solo resguarda la privacidad individual, sino que constituye un conjunto de derechos fundamentales interrelacionados que definen la relación entre el individuo y su información personal.

Finalmente, el análisis detallado del Código Orgánico Administrativo revela la importancia y el énfasis que se pone en la protección de la intimidad y los derechos personales

en el manejo de información por parte de entidades gubernamentales. Aunque el principio de protección de la intimidad se aplica específicamente a instituciones públicas, el procedimiento administrativo sancionador establece un marco riguroso para garantizar la transparencia, el respeto a los derechos fundamentales y la presunción de inocencia de los involucrados, la caducidad de la potestad sancionadora y los plazos de prescripción según la gravedad de las infracciones demuestran la voluntad del legislador de asegurar una conclusión oportuna de los procesos, evitando dilaciones innecesarias, así mismo, las garantías procesales, como la separación entre la función instructora y sancionadora, el derecho a ser notificado y la presunción de inocencia, refuerzan la protección de los derechos individuales en todo el procedimiento. En resumen, el Código busca equilibrar la necesidad de imponer sanciones con la salvaguarda de los principios fundamentales de justicia y respeto a la dignidad humana.

Recomendaciones

En atención a lo investigado:

Se recomienda el fortalecimiento de la Protección de Datos mediante la designación del Superintendente de Protección de Datos Personales, ya que sin la existencia de un organismo que determine sanciones pecuniarias importantes contra infractores, será muy poco probable que se asuman cambios en la recolección y uso de datos, esto implica establecer protocolos de seguridad más sólidos y fomentar una cultura de seguridad informática de datos en el sector bancario.

A pesar de que la regulación de protección de datos en Ecuador comenzó relativamente tarde, en comparación con sus pares, es esencial que todas las instituciones financieras cumplan estrictamente con la legislación actual, siendo imperioso que se determinen guías y estipulaciones por parte del defensor del cliente de los bancos, para procurar evitar sanciones.

Concienciación y Capacitación: Las instituciones financieras deben invertir en programas de concienciación y capacitación para su personal, con un enfoque en la importancia de la protección de datos y las mejores prácticas de seguridad.

Por otro lado, los usuarios también han de tomar medidas de seguridad adecuadas para proteger sus propios datos personales, lo que implica utilizar contraseñas seguras, estar alerta ante posibles signos de actividad sospechosa en sus cuentas financieras y en general regirse a una sana cultura de ciberseguridad.

Especialmente, en la futura Superintendencia de Protección de Datos Personales, se establezca un sistema denuncia eficaz para que los usuarios puedan informar sobre cualquier

vulneración de sus datos personales y tomar medidas rápidas para investigar y abordar tales incidentes.

Por parte de la sociedad civil y los grupos de defensa de los derechos, se debe fomentar la participación y la denuncia de problemas para ejercer presión hacia un cambio positivo además de promover la protección de datos y la responsabilidad de las instituciones financieras.

Estas recomendaciones buscan promover un entorno en el que se protejan adecuadamente los datos personales de los usuarios y se fomente la responsabilidad por parte de las instituciones financieras y las autoridades competentes en Ecuador. La protección de datos es esencial en la era digital y debe ser una prioridad tanto para el gobierno como para las empresas.

Referencias bibliográficas

AEPD. (2021). Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. *Agencia Española de Protección de Datos*. https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

AEPD. (2023). *Guía sobre el uso de las cookies*. Agencia Española de protección de datos. https://www.aepd.es/documento/guia-cookies.pdf

Aguilar Guzmán, A., Benites Estupiñán, E., Scotti, L., & SoroKin, P. (2022). La privacidad como Derecho Humano: Contribuciones para la promoción de una nueva agenda bioética. *«PATRIMONIO»: Economía Cultural y Educación para la Paz
 (MEC-EDUPAZ)*, *1*(21), 600. https://doi.org/10.22201/fpsi.20074778e.2022.1.21.77790

Álvarez, L. E. (2017). Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *Revista de Derecho*. https://repositorio.uasb.edu.ec/bitstream/10644/5945/1/05-TC-Enriquez.pdf

Arce, F. (2009). *El Habeas Data como garantia jurisdiccional e instrumento efectivo de la garantía del derecho a la privacidad en la Legislación Ecuatoriana* [Tesis previa a la obtención del titlo de Abogado, Universidad del Azuay]. https://dspace.uazuay.edu.ec/bitstream/datos/886/1/07511.pdf

Asamblea Nacional. (2021). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*.

Banco Pichincha. (2021). *Comunicado oficial a nuestros clientes: Incidente de ciberseguridad*. https://twitter.com/BancoPichincha/status/1447628963858296834?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1447628963858296834%7Ctwgr%5Efa275f3dc842c4ef57b495d227d45a23bc3104f8%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.elcomercio.com%2Factualidad%2Fnegocios%2Fbanco-pichincha-ciberseguridad-ciberataque-hackeo.html

Blume, I. (2021). Las nuevas tecnologías y la protección de datos en el entorno laboral: Retos y perspectivas legales. *THEMIS Revista de Derecho*, *79*, 435-449. https://doi.org/10.18800/themis.202101.025

Botero, C. (2012). EL DERECHO DE ACCESO A LA INFORMACIÓN EN EL MARCO JURÍDICO INTERAMERICANO. *Comisión Interamerica de Derechos Humanos*. https://www.oas.org/es/cidh/expresion/docs/publicaciones/acceso%20a%20la%20informacion%202012%202da%20edicion.pdf

Bureau of Justice Assistance. (1986). *Electronic Communications Privacy Act of 1986 (ECPA)*. BJA. https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#:~:text=The%20ECPA%2C%20as%20amended%2C%20protects,conversations%2C%20and%20data%20stored%20electronically

Cámara de Industrias y Producción. (2023, septiembre 11). SOBRE EL TRATAMIENTO DE DATOS PERSONALES: *CIP - Cámara de Industrias y Producción*. https://www.cip.org.ec/2023/09/11/sobre-el-tratamiento-de-datos-personales/

Carbonell, M., & Alexy, R. (Eds.). (2013). *El canon neoconstitucional* (1.ª ed.). Universidad del Externado de Colombia. https://doi.org/10.2307/j.ctv31zqgdm

Carrillo, F. N. R. (2021). Los ejes centrales de la protección de datos: Consentimiento y finalidad: Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador. *USFQ Law Review*, *8*(1), Article 1. https://doi.org/10.18272/ulr.v8i1.2184

CEPAL. (2022). Educación en tiempos de pandemia: Una oportunidad para transformar los sistemas educativos en América Latina y el Caribe. *Politicas Sociales* https://repositorio.cepal.org/server/api/core/bitstreams/e66c7b0e-41da-4a4a-be97-543097fccfb1/content

Chen Mok, S. (2010). Privacidad y protección de datos: Un análisis de legislación comparada. *Diálogos Revista Electrónica de Historia*, *11*(1), 111-152.

CISP. (2016). *Política de cookies*. https://developmentofpeoples.org/es/cookie-policy

Comisión Europea. (2018). *El Reglamento general de protección de datos*. Protección de datos en la UE. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es

Comité Jurídico Interamericano. (2021). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales*. Organización de los Estados Americanos. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Conde Ortiz, C. (2006). *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*. Servicio de Publicaciones de la Universidad de Cádiz. https://rodin.uca.es/handle/10498/26396

Cristea, L. (2017). *La protección de datos de carácter sensible en el Ámbito Europeo: Historia Clínica y Big Data en Salud* [Tesis Doctoral, Universidad Abat Oliba CEU]. https://www.tdx.cat/bitstream/handle/10803/442972/Tlcu.pdf?sequence=1

Diario Constitucional. (2018, junio 11). *Corte de Santiago confirma condena a Banco por infringir protección de datos de clientes.* Diario Constitucional. https://www.diarioconstitucional.cl/2018/06/11/corte-de-santiago-confirma-condena-a-banco-por-infringir-proteccion-de-datos-de-clientes/

Enríquez, O. A. M. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: Desafíos y cumplimiento. *Revista IUS*, *12*(41), 267-291.

EuropaPress. (2023, marzo 21). *Protección de Datos impone una multa de 70.000 euros a CaixaBank Payments & Consumer*. Europa Press.

https://www.europapress.es/economia/finanzas-00340/noticia-proteccion-datos-impone-multa-70000-euros-caixabank-payments-consumer-20230321190040.html

Ferrajoli, L. (2002). *Derechos y garantías*. Trotta S.A. https://www.te.gob.mx/formulario/media/files/4cd91799f6a2a69.pdf

Fiallos, A. V. (2017). Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa. *Foro: Revista de Derecho, 27*, Article 27.

García González, A. (2007). La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado. *Boletín mexicano de derecho comparado*, *40*(120), 743-778.

Gobierno de España. (2018). *Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.* BOE. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Gobierno de México. (2020). *México a la vanguardia con la nueva Ley Federal de Protección a la Propiedad Industrial*. https://www.gob.mx/se/prensa/mexico-a-la-vanguardia-con-la-nueva- ley-federal-de-proteccion-a-la-propiedad-industrial-256680?idiom=es#:~:text=%2D%20La%20Ley%20Federal%20de%20Protecci%C3%B3n,los%20retos%20de%20la%20innovaci%C3%B3n.

Godoy, L. N. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador. *Revista de Derecho, 27*

González, J. A. (2021, junio 2). Regulaciones | Protección de Datos para Entidades Financieras. *Sealpath*. https://www.sealpath.com/es/blog/regulaciones-proteccion-datos-entidades-financieras/

GOVERTIS, B. A. (2021, junio 16). Ecuador y su primera Ley Orgánica de Protección de Datos Personales. *Delegado de protección de datos*. https://dpd.aec.es/ecuador-y-su-primera-ley-

organica-de-proteccion-de-datos-personales

Herrera, J. A., & Fandiño, J. E. A. (2020). LA PROTECCION DE DATOS EN LA ERA DIGITAL COLOMBIA - ESPAÑA. *Revista Politécnico Grancolombiano*. https://alejandria.poligran.edu.co/bitstream/handle/10823/2142/Articulo%20Proteccion%20de%20datos%20%20en%20la%20era%20digita%20Colombia-Espa%C3%B1a%20Nov.%2029..pdf?sequence=1&isAllowed=y

INAI. (2015). *Manual en materia de seguridad de datos personales para MIPYMES y organizaciones pequeñas*. Instituto Nacional de Transparencia, Acceso a la información y Protección de datos personales.

INEC. (2022). *Encuesta Nacional de Empleo, Desempleo y Subempleo (ENEMDU), Junio 2022*. Gobierno de la Republica del Ecuador; Boletín Técnico N° 11-2022-ENEMDU. Encuesta Nacional de Empleo, Desempleo y Subempleo (ENEMDU), Junio 2022

López, C. (2013, febrero 27). Transparencia y acceso a la información en Ecuador. *Daniel López Carballo*. https://dlcarballo.com/2013/02/27/transparencia-y-acceso-a-la-informacion-en- ecuador/

Meraz Espinoza, A. I. (2018). Empresa y privacidad: El cuidado de la información y los datos personales en medios digitales. *Revista IUS, 12*(41), 293-310.

Meyer, T. (2004). *ANÁLISIS COMPARATIVO DE COOKIES Y LA PROTECCIÓN DE DATOS PERSONALES*. UNIVERSIDAD DE CHILE, FACULTAD DE DERECHO PARTAMENTO DE DERECHO PROCESAL. https://repositorio.uchile.cl/bitstream/handle/2250/107493/meyer_a2.pdf?sequence=3&isAllowed=y

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). *GUIA PARA TRATAMIENTO DE DATOS PERSONALES EN ADMINISTRACION PUBLICA*.

Acuerdo Ministerial 12. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2019/11/Gu%C3%ADa-de-protecci%C3%B3n-de-datos-personales.pdf

Núñez, E. J. A. (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*, Article 12-13.

Ordoñez, J. G. E. R. C. O. O. B. G. del C. (2019). *Constitucionalismo contemporáneo en América Latina*. Midac, Sl

Ordóñez Pineda, L., Correa Quezada, Andrea, Ordóñez Pineda, L., Correa Quezada, & Andrea. (2022). Políticas públicas y protección de datos personales en Ecuador: Reflexiones desde la emergencia sanitaria. *Estado & comunes, revista de políticas y problemas públicos*, *2*(15), 77-97. https://doi.org/10.37228/estado_comunes.v2.n15.2022.270

Organization of American States. (2012). *Ley de Modernización de los Servicios Financieros*. CUMPLIMIENTO DE REGULACIONES EN AMÉRICA: LEY GRAMM-LEACH-BLILEY (GLBA). https://www.entrust.com/es/digitalsecurity/hsm/solutions/compliance/americas/glba

Parlamento Europeo. (2023, marzo 31). *La protección de los datos personales*. Fichas temáticas sobre la Unión Europea. https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion- de-los-datos-personales

Pineda, L. O. (2019). El procedimiento de solicitud de adecuación de los datos de conformidad con la identidad de género. Reflexiones desde el derecho fundamental a la protección de datos. *Foro: Revista de Derecho*, *32*, Article 32. https://doi.org/10.32719/26312484.2019.32.10

Plua, G. E. (2017). El Derecho al olvido en la era digital. El caso de Google en España y El Tiempo en Colombia. *Foro: Revista de Derecho*, *27*, Article 27.

Ramírez, J. (2023, junio 15). Las Implicaciones Legales de las brechas de Ciberseguridad. *In Solidum Abogados*. https://insolidumabogados.com/las-implicaciones-legales-de-las-brechas- de-ciberseguridad/

Redacción Expreso. (2023). Lasso envía terna para Superintendencia de Protección de Datos. *EXPRESO*. https://www.expreso.ec/actualidad/economia/lasso-envia-terna-superintendencia-proteccion-datos-177150.html

Redrobán Barreto, W. E. (2023). Protección de datos personales en Ecuador a consecuencia de la emergencia sanitaria Covid-19. *Revista Universidad y Sociedad*, *15*(2), 194-206.

Russel. (2023, julio 18). Ley de Protección de Datos Personales en Ecuador. *Russell Bedford EC*. https://russellbedford.com.ec/ley-de-proteccion-de-datos-personales-en-ecuador/

Sánchez, M. I. (2015). LIBERTAD INFORMÁTICA Y PROTECCIÓN DE DATOS: DESARROLLO EN LA JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL Y TUTELA PENAL EN EL DELITO DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS. *Anuario Iberoamericano de Justicia Constitucional*, *19*, 323-363 https://doi.org/http//:dx.doi.org/10.18042/cepc/aijc.19.12

Santander. (2023). *Data protection policy | Santander Bank*. https://www.santander.com/en/landing-pages/data-protection-policy}

Superintendencia de Bancos. (2022). *Proyecto de Norma: Protección y Defensa de los Derechos del Usuario Financiero de las Entidades de los Sectores Financieros Público y Privado*. RESOLUCIÓN No. SB-2019-. https://www.superbancos.gob.ec/bancos/wp- content/uploads/downloads/2019/12/Norma-Protecci%C3%B3n-Usuarios.pdf

Suprema Corte de Justicia de la Nación. (2018). *Criterios del poder judicial de la Federación*

en materia de Protección de Datos Personales y otros componentes relacionados. Sistema Bibliotecario de la Suprema Corte de Justicia de la Nación. https://www.scjn.gob.mx/sites/default/files/pagina_transparencia/documento/2018-11/CriteriosPJF_Proteccion_Datos_2a_Ed_Digital_2018.pdf

Tribunal Constitucional de España. (2002). *EL DERECHO A LA PROTECCIÓN DE DATOS Y EL RGPD*. Directiva 97/66/CE del Parlamento Europeo y del Consejo. https://www.dpoitlaw.com/reglamento-general-de-proteccion-de-datos-rgpd/unidad-i-1-introduccion/

Zambrano, R. (2022). ¿Cuál es el perfil de un delegado de protección de datos?, especialización que tendrá gran demanda por parte de las empresas en Ecuador. *El Universo*. https://www.eluniverso.com/noticias/informes/cual-es-el-perfil-de-un-delegado-de-proteccion-de- datos-especializacion-que-tendra-gran-demanda-por-parte-de-las-empresas-en-ecuador-nota/

Zamora, F. J. T. (2010). ESPECIALIZACION EN DERECHO PROCESAL. *DSpace*. https://dspace.uazuay.edu.ec/bitstream/datos/6634/1/07613.pdf