FACULTAD DE POSTGRADOS

MAESTRÍA EN DERECHO DIGITAL E INNOVACIÓN

TÍTULO DE LA INVESTIGACIÓN

Aplicación del bloqueo o anonimización de datos personales en consumidores bancarios, como parte del derecho de eliminación determinado en la normativa en materia de protección de datos personales, en el Ecuador.

Profesor

Roberto Lara

Lorena Naranjo Godoy

Autores

Geovanny David Ayala Carrasco

Christian Gabriel Portero Jerez

2024

Resumen Ejecutivo

Con la expedición y vigencia de la Ley Orgánica de Protección de Datos Personales, el derecho a la eliminación ha generado en las entidades bancarias la necesidad de establecer procesos técnicos y operativos que garanticen su ejercicio, sin que estos se contrapongan a las disposiciones normativas especializadas en materia financiera. Por ello, esta investigación presenta un proyecto de resolución sobre anonimización y bloqueo de datos personales expedida por la autoridad competente, junto con un manual de procedimiento de anonimización y bloqueo; lo cual, a más de resolver la problemática puntual de la presente investigación, pueda ser un marco de referencia para las demás industrias con esta problemática. En este sentido, a través de encuestas y entrevistas realizadas a expertos en la materia que estén vinculados al sector financiero, así como análisis comparado de otras legislaciones, se pudo concluir que el sector bancario ha dado pasos importantes para garantizar la seguridad de la información de sus clientes; sin embargo, requieren reforzar sus procesos para adecuarlos a la normativa vigente en materia de protección de datos personales, más aún cuando su oferta financiera se sustenta en la prestación de un servicio de orden público, que genera gran trascendencia en la sociedad.

Abstract

With the enactment and enforcement of the Organic Law on Personal Data Protection, the right to deletion has generated the need for financial institutions to establish technical and operational processes that guarantee the exercise of this right, without compromising the observance of specialized financial regulations. This research presents a draft regulation addressing anonymization and blocking of personal data to be issued by authorities, along with a procedural manual for anonymization and blocking. This not only addresses the very issue of the research at hand but could well serve as a reference framework for other industries facing the same issue. Through interviews with experts in the field who are linked to the financial industry as well as a comparative analysis of foreign legislations, it was concluded that the banking sector has taken important steps towards ensuring the safety of its clients´ information; however, it is essential to strengthen its processes in order to comply with data protection regulations, especially since its services are of a public nature, thus of great impact on society.

A mi esposa y a mi hija, gracias por su amor,
paciencia y comprensión en cada momento del camino.
A mis padres y hermanas, por compartir conmigo la vida.
(Christian P.)

A mis padres, si ustedes conmigo, nadie contra mí.
A mi hermano, por su apoyo incondicional
en cada objetivo planteado.
(David A.)

Índice de Contenido

Lista de Anexos

Introducción

La Constitución de la Republica del Ecuador (R.O. 449 del 20 de octubre de 2008), refiere en su artículo 92 sobre el derecho de los ciudadanos al acceso a los documentos y datos personales que existan sobre si mismos, y conocer sobre el uso que se den a estos. Dicho sustento normativo guarda plena armonía con el derecho a la protección de datos de carácter personal determinado por el artículo 66 numeral 19 ibidem, lo cual nos permite entender que el estado ha pretendido garantizar la protección de la privacidad de las personas en lo referente a su información personal, sea esta pública o privada.

Desde este antecedente general, se determina que la legislación ecuatoriana ha mantenido durante los últimos treinta años ciertos esbozos normativos en materia de protección de datos personales en instituciones bancarias, tal es así que la Ley General de Instituciones del Sistema Financiero, (Congreso Nacional, 1994), ya especificaba definiciones sobre sigilo y reserva bancaria respecto la información crediticia de los clientes de las entidades financieras, lo cual se mantiene con el vigente Código Orgánico Monetario y Financiero.

Con ello, al focalizarse en el adecuado tratamiento y custodia de la información personal de consumidores financieros, se observa que el artículo 225 del Código Orgánico Monetario y Financiero (2014), establece la obligatoriedad para las entidades que conforman el sistema financiero nacional, de mantener sus archivos contables físicos, incluyendo los respaldos contables relativos a las operaciones financieras es estos, por el plazo de diez años contados a partir de la conclusión de la operación correspondiente y por quince años en el formato digital autorizado por las superintendencias (Asamblea Nacional del Ecuador, 2014).

Es así como, con la expedición de la Ley Orgánica de Protección de Datos Personales en mayo de 2021, y su reglamento de aplicación en noviembre de 2023, se han generado nuevos retos para personas jurídicas públicas, privadas e industrias, respecto al tratamiento y protección de datos

personales. El artículo 15 de dicha ley habla sobre el derecho de eliminación que tienen los titulares; mientras que el artículo 9 de su reglamento de aplicación le otorga al responsable la facultad de eliminarlos, bloquearlos o anonimizarlos (Asamblea Nacional del Ecuador, 2021; Presidencia de la República del Ecuador, 2023).

Lo mencionado en el párrafo anterior resulta un tanto confuso al momento de encontrar coherencia entre ambas normas de materia especial; pues al parecer no existe una adecuada vinculación entre el derecho a la eliminación de datos personales y la obligación de custodia de soportes contables y transaccionales; motivo por el cual, es necesario comprender detalladamente el contexto de estos preceptos jurídicos.

Es así como, con la vigencia del Reglamento General de la Ley Orgánica de Protección de Datos Personales, se ha podido comprender de cierta manera, aunque un tanto confusa, aquellos aspectos imprecisos sobre el derecho de eliminación; incorporando ciertos términos no previstos en la Ley, como el bloqueo o anonimización de datos, pero que indudablemente genera dudas sobre sobre su aplicación, así como contradicciones al momento de hacer efectivo dicho derecho constitucional de los ciudadanos.

Identificación del Objeto de Estudio

1. Planteamiento del Problema

1.1. El Problema

La falta de criterios jurídicos oportunos, así como normativa insuficiente para aplicar el bloqueo o anonimización de datos personales en consumidores financieros, como parte del derecho de eliminación establecido por la Ley Orgánica de Protección de Datos Personales y su reglamento aplicación, genera interpretaciones imprecisas o subjetivas frente a la obligatoriedad de las entidades financieras de respaldar o mantener la información sobre operaciones financieras, determinada por el artículo 225 del Código Orgánico Monetario y Financiero y demás normativa especializada.

1.2. Pregunta General de Investigación

¿Que debe contener una resolución emitida por la autoridad administrativa competente para garantizar en el derecho de eliminación, el bloqueo o anonimización de datos personales de consumidores bancarios y como las entidades financieras la deben aplicar?

1.3. Preguntas específicas de investigación

2. ¿Cómo se regula al derecho de eliminación de datos personales, en la legislación ecuatoriana?
3. ¿Cómo se vincula el bloqueo o anonimización de datos al derecho de eliminación de Datos Personales de los consumidores bancarios?
4. ¿Cuál es el proceso que debe seguir la institución bancaria, para el correcto ejercicio del bloqueo y/o anonimización de datos personales de sus clientes?
5. ¿Cómo regularía la Autoridad de Protección de Datos, el bloqueo o anonimización de datos personales como parte del derecho de eliminación de los consumidores bancarios?

1.4. Efectos del problema

La violación del derecho de eliminación, bloqueo o anonimización de Datos Personales de los consumidores bancarios, sin la valoración jurídica

pertinente acarrea una violación expresa a la norma que regula la materia, lo cual podría generar sanciones administrativas o pecuniarias por parte de los entes de control, así como procesos de carácter judicial.

1.5. Causas del Problema

La falta de designación de la autoridad de protección de datos, que provoca a su vez la inexistencia de normativa y políticas, que determine la aplicación del derecho de eliminación, bloqueo o anonimización de Datos Personales de los consumidores bancarios, cuyo incumplimiento podría conllevar una violación expresa a los derechos de los consumidores de servicios bancarios, lo cual derivaría en sanciones administrativas o pecuniarias por parte de los entes de control, así como procesos de carácter judicial.

Revisión de la Literatura

1. Marco Conceptual

1.1. Antecedentes y fundamentos jurídicos sobre el derecho de eliminación de datos personales en la legislación ecuatoriana.

Capítulo I

Derecho de eliminación de datos personales en la legislación ecuatoriana

La protección de datos personales no es un término nuevo en Ecuador, ya que la Constitución del 2008 reconoce y garantiza derechos sobre la protección de la información personal y la privacidad, estudiados desde varios campos para garantizar su amparo; pero el avance tecnológico y exponencial crecimiento de la sociedad de la información mediante sus plataformas, teorías y herramientas ha complicado la adecuada garantía de estos derechos, lo que incluso evidenció riesgos de delitos informáticos sobre la información de los ciudadanos que no tiene las medidas de resguardo necesarias.

Este antecedente coincide, con aquellas disposiciones que determinaba la derogada Ley Orgánica de Transparencia y Acceso a la Información Pública de 2004, y a posterior, en igual manera superficial, con cuerpos normativos aún vigentes, orientados a la protección de datos recopilados en fuentes públicas, como la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, que en su parte pertinente determina el procedimiento para el ejercicio del Habeas Data, como un mecanismo efectivo para el ejercicio del derecho fundamental del titular a acceder a su información personal y obtener su eliminación o corrección si esta fuera incorrecta, imprecisa o falsa (Asamblea Nacional del Ecuador, 2009, arts. 49 - 51). Así como la Ley Orgánica de Gestión de la Identidad y Datos Civiles, que tiene por objeto garantizar el derecho a la identidad de las personas y la protección de sus datos de carácter civil (Asamblea Nacional del Ecuador, 2015, art. 1).

A pesar de la vigencia de normas y el saturado conglomerado de derechos consagrados en la Constitución, el país se enfrentó a una de las más escandalosas fugas de información personal de los ciudadanos, pues en el año 2019 se identificó una brecha de seguridad a los servidores de la empresa Novastratech S.A, respecto a los datos personales de aproximadamente veinte millones de ecuatorianos, entre los que constaba información de personas fallecidas; en este sentido, el artículo de prensa publicado por Diario El Comercio el 16 de septiembre de dicho año, nos explica que esta filtración incluía información sumamente sensible, como son datos relativos a la identidad de las personas, números telefónicos, direcciones domiciliarias, información relativa a la educación de estos, datos crediticios y financieros, entre otros (El Comercio, 2016), sumado a que el hallazgo fue realizado por la empresa extranjera *vpnMentor*.

En este sentido, comprendemos que la evidencia aquí descrita resulta escandalosa por la ausencia de mecanismos de seguridad o protocolos de protección oportunos, que garanticen la inviolabilidad o custodia de la

información que manejaba *Novastratech*, más aún cuando sus servidores se encontraban en la ciudad de Miami de los Estados Unidos de América, lo que alerta de los riesgos asociados a este hecho de gran magnitud, como delitos informáticos relativos a estafa, así como ciberataques, espionaje o robo de dinero, los expertos informáticos que descubrieron está anomalía fueron *Noam Rotem* y *Ran Lokar* (Córdova, 2023, p. 2).

Este antecedente fáctico generó preocupación en los entes estatales que administran datos de los ciudadanos, así como entidades privadas encargadas de similar gestión, por lo que se presenta a revisión del legislativo el proyecto de Ley Orgánica de Protección de Datos Personales, cuya finalidad pretende regular de manera específica, clara y objetiva la administración de la información de las personas, así como el ejercicio de los derechos que de estos actos derivan.

A su vez con la emergencia sanitaria declarada en el país debido a la pandemia del Covid-19, se volvió más frecuente el uso de plataformas digitales, entre ellas el comercio electrónico, banca móvil y demás canales no presenciales, en los cuales existía la interacción masiva de datos personales, muchos eran de carácter sensible, para la prestación de productos y servicios varios, entre ellos los financieros, los cuales no contaban con los mecanismos y protocolos adecuados para su protección.

En este sentido, de acuerdo con el artículo denominado "*Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria*", publicado por Ordoñez Pineda, Correa Quezada y Correa Conde (2022) donde resaltan la ausencia de normativa especializada en la protección de la información personal en el contexto de este acontecimiento mundial, pero también analiza la creación y aplicación emergente del Decreto Ejecutivo No. 1017 del 17 marzo de 2020, como un mecanismo de monitoreo y seguimiento de las personas para la adopción de medidas administrativas o judiciales, al permitir el uso de "*plataformas satelitales y de telefonía móvil para monitorear la ubicación de personas en*

estado de cuarentena sanitaria y/o aislamiento obligatorio… a fin de ponerlas a disposición de las autoridades judiciales y administrativas competentes" (Presidencia de la República del Ecuador, Decreto Ejecutivo No. 1017, 2020, art. 11).

Resultaba escandaloso para la sociedad pensar que el Ejecutivo permita la vulneración de un derecho fundamental como la vida privada de las personas, sin embargo, la emergencia sanitaria del COVID-19 impactó significativamente el ejercicio de varios derechos fundamentales, entre los cuales se encuentran el acceso a la salud, alimentación, educación, libre circulación, etc., exacerbado las desigualdades existentes y dando lugar a nuevas vulneraciones de los derechos.

Así mismo, debe considerarse lo señalado por los tratadistas Amoroso, Bárzaga y Fabelo (2020, citados por Ordoñez Pineda et al., 2022), indicando que:

> No se trata de dejar de hacer uso de la tecnología y de limitar el tratamiento de datos como es el caso del monitoreo de las personas contagiadas por la emergencia sanitaria, por medio de las plataformas satelitales y de telefonía móvil, sino, que se respeten la garantía de protección de datos y, en suma, la vida privada de las personas. Además, entendiendo que la información relativa a la salud constituye una serie de datos muy sensibles, debe evitarse posibles discriminaciones e intromisiones ilegítimas que afecten a la intimidad y el derecho a la integridad personal de los pacientes. (p. 83)

Lo señalado en esta cita textual, consolida la situación que atravesaba el Ecuador previo el advenimiento de la pandemia y posterior con los hechos de emergencia generados, resaltando la necesidad de normar el derecho de protección a la privacidad de las personas, mediante un tratamiento oportuno, sistematizado, y garantista.

No fue hasta la promulgación de Ley Orgánica de Protección de Datos Personales (en adelante LOPDP) en el 2021, que se estableció un régimen común para garantizar el ejercicio del derecho constitucional especificado en

el Articulo 66 numeral 19, que además incluye el acceso, decisión y protección de dichos datos, desarrollando principios, derechos, obligaciones y un mecanismo de tutela; pues es esencial que toda persona conozca las circunstancias que van a rodear el tratamiento, destino y eliminación de sus datos, con el fin último de manifestar su consentimiento de una manera libre, informada y con pleno conocimiento de causa (Ayuso, 2019, pp. 27–74).

Es importante que el legislativo haya normado estos derechos, pues se constituye como un avance importante en la protección de los derechos de las personas, quienes no estaban familiarizados con el uso que las instituciones estatales o privadas daban a sus datos, empoderando a las personas en el control de su información.

Al referirnos sobre los derechos derivados de la protección de datos personales, nos encontramos con conceptos técnicos y jurídicos que permiten plasmar la teoría del ejercicio de la privacidad; como son el acceso, rectificación, cancelación y oposición de datos personales de los titulares, doctrinariamente conocidos como derechos ARCO. Sin embargo, la Asamblea Nacional del Ecuador amplio estos derechos, estableciendo además los de anulación, portabilidad y eliminación.

Sobre esto, la normativa europea la define como derecho de supresión, mientras que la mexicana como derecho de cancelación, estableciendo varias y diferentes circunstancias para su aplicación; sin embargo, comparten como objetivo similar, el suprimir los datos personales cuando concurra alguna de las circunstancias con el fin último de cese en el tratamiento por parte del responsable.

En Ecuador la Ley Orgánica de Protección de Datos Personales define al derecho de eliminación en su artículo 15 como “*el titular tiene el derecho a que el responsable del tratamiento elimine sus datos personales*…” (Asamblea Nacional del Ecuador, 2021, art. 15, inc. 1), sin embrago, la Corte Constitucional en la Sentencia No. 1868-13-EP/20 (08 de julio de 2020) amplió la definición del derecho de eliminación como la acción de suprimir la

información de carácter personal que está en registros, archivos, documentos o cualquier base de datos ya sea privada o pública, lo que implica desaparecer la información ya sea física o digital e impedir su recuperación. Si bien la expedición de la mencionada Ley y la Sentencia son disparejas, la segunda amplia el contenido y las características del derecho de eliminación.

Pero debe considerarse que existe otras denominaciones y definiciones para el conocido derecho de eliminación, para esto debe realizarse un análisis comparado de definiciones en otras legislaciones, ya que si bien la ley manda no enseña (*lex iubeat, non docet*), el empleo de definiciones puede cambiar el alcance de aplicación de la norma o determinar características propias del derecho en relación a otros similares pero no iguales, por ejemplo en Ecuador la eliminación, el bloque y la anonimización tiene el mismo fin pero distintas formas de aplicación.

En México la Ley Federal de Protección de Datos Personales en Posesión de Particulares del 5 de julio de 2010 llama en su artículo 25 a la acción de eliminar datos personales como Derecho de Cancelación, definiéndola como la acción por la cual el titular puede solicitar la supresión de sus datos personales, la cual no es instantánea sino tiene un paso previo que es el bloqueo de datos, por el tiempo de prescripción de las acciones, únicamente de archivos privados por el contexto de la ley (Cámara de Diputados del Honorable Consejo de la Unión, 2010). Así también en México el Reglamento de aplicación de la Ley define al derecho de cancelación como la "*Actividad consistente en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas por el responsable*." (Presidencia de los Estados Unidos Mexicanos, 2011, art. 2 núm. 12). Más allá de la terminología, la diferencia sustancial radica en que la legislación mexicana concibe la cancelación como un proceso de dos etapas, bloqueo y supresión, durante el bloqueo se aplica por el tiempo de prescripción de las acciones, sin embargo, los datos se conservan, pero se restringe su tratamiento, transcurrido ese

plazo, se procede a la supresión definitiva. Esta aproximación contrasta con la normativa ecuatoriana, donde el bloqueo no se plantea como un paso previo a la eliminación, sino como una alternativa viable cuando la supresión inmediata no es posible por motivos legales o contractuales. Este caso ilustra como la regulación del derecho de eliminación, aunque persiga un objetivo similar, puede variar significativamente en su implementación y práctica.

Por otro lado, el Parlamento Europeo asocia el derecho de eliminación o cancelación con el derecho al olvido y lo ha denominado Derecho de Supresión, el Reglamento (UE) 2016/679 del 27 de abril de 2016 establece que "*El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos*…" (art. 17), si bien se requiere circunstancias como ya no ser útiles para el tratamiento o que el titular haya retirado el consentimiento no establece un periodo de bloqueo como la legislación mexicana, aunque tampoco distingue los archivos de los cuales puede eliminarse como en Ecuador. Así también cabe mencionar que en Europa mediante Directiva 95/46 de 24 de octubre de 1995 no se definía ni establecía al derecho de supresión como un derecho autónomo sino como parte del Derecho al Acceso, el artículo 12 literal b) de la menciona norma solo permitía la eliminación cuando existía causas que justifiquen violaciones a la Directiva o datos inexactos o incompletos (Parlamento Europeo y Consejo de la Unión Europea, Directiva 95/46, 1995).

Como se puede observar las legislaciones europea, mexicana y ecuatoriana definen al derecho eliminación, cancelación o supresión como derechos autónomos y empleando formas de tratamiento asociadas a borrar, eliminar o destruir datos personales con el fin de evitar la identificación de su titular o la capacidad de recuperar la información, solo la legislación mexicana emplea dos acciones de tratamiento para definir su llamado derecho a la cancelación, es decir usa las formas de bloqueo y supresión, mientras que Europa solo da contenido con tratamientos de supresión sin permitir otras

acciones extras y Ecuador crean al derecho de eliminación como autónomo con acciones como el bloqueo o anonimización que le son sustitutivas.

Sin embargo, existen excepciones para el ejercicio del derecho de eliminación las cuales deben ser interpretadas de manera restrictiva para garantizar la protección efectiva de los derechos de los titulares de los datos, una de ellas es que exista una obligación legal de conservarla (Reglamento de la Ley Orgánica de Protección de Datos Personales [RLOPDP], art. 9). Un ejemplo claro de esto es lo establecido en el artículo 225 del Código Orgánico Monetario y Financiero (2014), cuyo texto establece que toda entidad que conforme el sistema financiero nacional, mantendrá sus archivos contables físicos, incluyendo los respaldos respectivos, por el plazo de diez años contados a partir de la conclusión de la operación correspondiente y por quince años en el formato digital autorizado por las superintendencias (Asamblea Nacional del Ecuador, 2014). En este caso, existe una disposición legal que permite a las instituciones financieras mantener archivos por más tiempo, incluso pese a la petición de eliminación realizada por el titular.

En este sentido, el presente estudio se centra en el derecho de eliminación, establecido en el artículo 15 de la Ley Orgánica de Protección de Datos Personales y artículo 9 de su Reglamento de aplicación, que permite considerar algunas alternativas como el bloqueo o anonimización, para la efectiva aplicación de este derecho.

Capítulo II

1.2. El bloqueo o anonimización de datos personales dentro del derecho de eliminación establecido en la normativa local y comparada

La normativa en materia de protección de datos personales de Ecuador establece algunas alternativas para la efectiva aplicación del derecho de eliminación cuando, según el RLOPDP, obliga al responsable a "*proceder con la eliminación, bloqueo o anonimización de los datos en su posesión*" (Presidencia de la República del Ecuador, 2023, artículo 9); disposición que no realiza mayor distinción entre estas dos figuras, anonimización o bloqueo,

sin embargo los liga con el interés legítimo del responsable, con la obligación legal de conservación y con la finalidad del tratamiento de datos personales.

Al hablar del interés legítimo del responsable del tratamiento de datos, hablamos de la facultad que permite a una institución, organización, empresa o entidad procesar datos personales cuando existe autorización o motivo justificado, para justificarlo el responsable debe hacer un examen de ponderación de intereses, en el que pese su interés legítimo frente a los derechos y libertades del interesado. La ponderación implica sopesar individual y cuidadosamente los intereses en juego y determinar cuál debe prevalecer en las circunstancias específicas del caso, considerando el nivel de protección y las medidas de seguridad que se deben aplicar.

En la legislación ecuatoriana, según la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, los Jueces Constitucionales eran los únicos que en su momento podían ponderar, entre los principios y normas, solo *"cuando mayor sea el grado de la no satisfacción o de afectación de un derecho o principio, tanto mayor tiene que ser la importancia de la satisfacción del otro*" (Asamblea Nacional del Ecuador, 2009, art. 3 inc. 2 núm. 3) Actualmente, la ponderación se aplica tanto en el ámbito judicial como en el administrativo, tanto es así que, el Reglamento General de la Ley Orgánica de Protección de Datos Personales permite la evaluación del interés legítimo del responsable del tratamiento o del tercero interesado que deberá ser necesario y proporcionado (Presidencia de la República del Ecuador, 2023, art. 7).

En cuanto a la obligación legal de conservación, la normativa establece que las empresas y organizaciones que traten datos personales solo pueden conservarlos durante un período no superior al necesario para los fines que justificaban el tratamiento. Pero la misma norma establece excepciones para ejercer el derecho de eliminación, las cuales deben interpretarse de manera restrictiva para garantizar la protección efectiva de los derechos de los titulares de los datos (Presidencia de la República del Ecuador, RLOPDP, 2023, art. 9). Un ejemplo es el plazo establecido por el Código Orgánico Monetario y

Financiero (2014) que toda entidad financiera debe cumplir, pues sus archivos contables, incluyendo los respaldos respectivos, deben conservarse por diez años contados tras la conclusión de la operación y quince años en el formato digital autorizado por las superintendencias (Asamblea Nacional del Ecuador, 2014, art. 225). Como se puede evidenciar, existe una disposición legal en la norma especializada del sistema financiero nacional que permite a las instituciones financieras conservar archivos por más tiempo, que el permitido en la legislación de datos personales.

Otra de las características generales del bloqueo y anonimización establecidos en el Reglamento de la Ley Orgánica de Protección de Datos Personales (Presidencia de la República del Ecuador, 2023, artículo 9) es la finalidad del tratamiento de datos, la cual está ligado de manera directa al principio de la conservación de la LOPDP, que en síntesis establece que "l*os datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento"* (Asamblea Nacional, 2021, art. 10, lit. i) además obliga que el responsable del tratamiento junto con el encargado del tratamiento debe establecer plazos para su supresión o revisión periódica, como garantía de no conservación del más tiempo del necesario.

En la legislación española, la conservación no es un principio, pero igual que en la legislación ecuatoriana su objetivo es el mismo, que los datos personales deben conservarse durante un período no mayor al necesario para los fines para los que se recopilan y tratan, además le correspondería al responsable junto con el encargado establecer de manera contractual, cuando finalice la prestación de los servicios, sobre su destrucción o devolución, en su caso, a un nuevo encargado, salvo previsión legal en contrario según la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (Jefatura del Estado de España, 2018, art. 33). Como se puede evidenciar la conservación de datos personales es un principio fundamental en la normativa de protección de datos de España,

México y Ecuador. Este principio establece que las empresas y organizaciones solo pueden conservar datos personales durante un período no superior al necesario para los fines para los que se recopilaron y se tratan, sin embargo, divergen en como los titulares deben ejercer este derecho y sobre que otras alternativas se pueden aplicar cuando una normativa no permita su eliminación.

1.2.1. Bloqueo de Datos.

La Ley Orgánica de Protección de Datos Personales (2021) dispone en su artículo 15 que los titulares de datos personales pueden ejercitar el derecho de eliminación, este artículo si bien describe supuestos no determina el contenido para su aplicación, en su lugar crea una confusión con otras acciones de tratamiento de datos, ya que su inciso final agrega "*el responsable del tratamiento de datos personales implementará métodos y técnicas para eliminar, hacer ilegible, o dejar irreconocibles de forma definitiva y segura los datos personales…*" (Asamblea Nacional del Ecuador, 2021, art. 15, inc. 3), determinando que la supresión no es la acción inequívoca de este derecho subjetivo, sino que puede efectivizarse con otras acciones, dependiendo de los términos del contrato o los llamados intereses legítimos del artículo 7 de la mencionada Ley.

El Reglamento de la Ley Orgánica de Datos Personales (Presidencia de la República del Ecuador, 2023, arts. 9 y 11) como alternativas a la eliminación, establece que estos también pueden bloquearse. Debe entenderse que el bloqueo es la conservación de los datos personales en un archivo físico o digital, pero restringiendo su acceso, permitiendo que solo personas autorizadas tengan acceso a los datos (Instituto Interamericano de Cooperación para la Agricultura, 2023). El bloqueo hace ilegible o deja irreconocible cualquier dato personal, si se cumplen los supuestos taxativos del artículo 15 de la ley orgánica, es cuando es imposible borrar las bases de datos o cuando se presente un requerimiento de eliminación, rectificación, etc., entonces se presenta como una acción suplementaria cuando el

responsable del tratamiento no está facultado o justifica la necesidad de conservarlas.

La legislación mexicana establece al bloqueo, como un período de tiempo en el cual el dato ya sea por culminación del plazo de prescripción legal o contractual, no podrá ser objeto de tratamiento, transcurrido este período se procederá a su cancelación y posterior supresión en la base de datos que corresponda, según la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Cámara de Diputados del Honorable Consejo de la Unión, 2010, arts. 3 y 25). Esto en concordancia al Reglamento de la Ley Federal de Protección de Datos Personales en posesión de los Particulares que establece que el "*propósito del bloqueo es impedir el tratamiento, a excepción del almacenamiento, o posible acceso por persona alguna*" (Presidencia de los Estados Unidos Mexicanos, 2011, art. 108), siempre y cuando no exista disposición legal que prevea lo contrario. Como podemos apreciar, en la legislación mexicana, la figura del bloqueo se utiliza como una medida temporal de carácter cautelar, restringiendo su tratamiento, mas no su almacenamiento, con el fin último de suprimir el dato, siempre y cuando sea por culminación del plazo de prescripción legal o contractual.

Al igual que la mexicana, la normativa española ha desarrollado de una manera clara al bloqueo y su aplicación, estableciendo cinco numerales en los cuales destacan, que el bloqueo se puede aplicar únicamente cuando proceda la rectificación o supresión, excepto cuando se tiene que poner a disposición de autoridades administrativas, fiscales o judiciales para la exigencia de posibles responsabilidades derivadas del tratamiento, transcurrido ese plazo deberá procederse a la destrucción de los datos. Además, establece que la Agencia Española de Protección de Datos y las autoridades competentes de protección de datos podrán reglar excepciones al bloqueo (Jefatura del Estado de España, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, 2018, art. 32).

En Ecuador, no se ha establecido ni definido la figura del bloqueo, pero, según la legislación comparada más desarrolla que la nuestra, se puede establecer como una medida de seguridad temporal que permite restringir el tratamiento de datos personales, impidiendo que accedan, modificaran o utilicen terceros. Al ser temporal, el responsable del tratamiento podrá conservar los datos bloqueados durante el tiempo necesario para cumplir con sus obligaciones legales o para resolver la reclamación del titular.

1.2.2. Anonimización de Datos.

La Agencia Española de Protección de Datos, define a la anonimización de datos como "*el conjunto de buenas prácticas y técnicas que reducen el riesgo de identificación de personas*", sin embargo, señala que es complejo garantizar la anonimización absoluta, por lo que el riesgo de reidentificación se aborda como un riesgo residual, asumido y gestionado, y no como un incumplimiento de la normativa. Es decir, cubre tanto el objetivo de anonimización, como el de mitigación del riesgo de reidentificación, el cual aumenta con el paso del tiempo, debido a la posible aparición de nuevos datos o el desarrollo de nuevas tecnologías. (Secretaria de Estado de Digitalización e Inteligencia Artificial de España, 2022).

En este sentido, encontramos un primer antecedente cercano en el año 2019, cuando el Ministerio de Telecomunicaciones y Sociedad de la Información expidió la Guía para el tratamiento de datos personales en la administración pública, promulgada en el Registro Oficial No. 18 del 15 de agosto de 2019, donde se define a la anonimización de manera similar al Reglamento de Protección de Datos de la Unión Europea, como el proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere (Parlamento Europeo y el Consejo de la Unión Europea, Reglamento (UE) 2016/679, 2016).

Así mismo el artículo 9 del Decreto Ejecutivo No. 904 (Presidencia de la República del Ecuador, 2023) dispone la posibilidad de anonimizar datos entendiendo otra medida distinta a la eliminación como la ha definido la Corte

Constitucional. La anonimización consiste en el proceso de cambiar los datos personales del titular por datos anonimizados cambiando los caracteres que componen la información, pero manteniendo las bases de datos originales para futuros procesos de reidentificación (Agencia Española de Protección de Datos, 2022). La anonimización se convierte en otro proceso sustitutivo del derecho de eliminación porque rompe el vínculo entre el dato personal y la identificación del titular, si bien no elimina la base de datos porque es necesario el proceso de reidentificación justificando en un interés legítimo y lícito del Responsable del tratamiento, si permite al igual que el bloqueo, la imposibilidad de que una persona no autorizada o el público (con bases de datos públicas) puedan identificar al titular atentando contra su derecho a la intimidad u honor, momentáneamente.

Otro de los antecedentes jurídicos relevante sobre la anonimización se encuentra en la Guía de datos abiertos aplicación en administración pública central, expedida mediante Acuerdo Ministerial 35, y publicada en el Registro Oficial Suplemento 371 del 15 de enero de 2021; en cuyo documento encontramos criterios para el acceso a dichos datos, garantizando la debida tutela de los derechos de los titulares. En este sentido, el estado a través de sus entidades públicas considera a la anonimización como un mecanismo de protección de datos personales de los ciudadanos impidiendo su identificación. Igualmente, se determinan lineamientos para una adecuada disociación, y técnicas a aplicarse para este proceso.

La anonimización se define como un proceso estratégico de manipulación de datos que implica la eliminación o modificación de información personal de individuos o entidades. Su objetivo es evitar que se identifiquen directa o indirectamente a partir de los datos derivados. Este método se emplea para resguardar la privacidad y confidencialidad de la información personal. Asimismo, persigue alcanzar un equilibrio entre preservar la privacidad y la utilidad de los datos, garantizando una gestión segura y ética de la información.

Si bien la anonimización se presenta como un mecanismo robusto para proteger la privacidad, el auge del Big data e inteligencia artificial plantean nuevos desafíos, pues la capacidad de esta tecnología para analizar grandes conjuntos de datos y encontrar patrones ocultos, pueden socavar la efectividad de la anonimización. Por ejemplo, algunos algoritmos de aprendizaje automático podrían utilizarse para re identificar a los individuos a partir de los datos anonimizados mediante la corrección con otras fuentes de información públicamente disponibles.

La relevancia de este proceso se manifiesta por las inquietudes éticas y legales relacionadas con la protección de los datos personales y, en consecuencia, con su privacidad. En ese sentido, Milanes (2017) establece que "*el desarrollo de fenómenos como el Big Data, el internet de las cosas, la decisión algorítmica, el aprendizaje automático o la inteligencia artificial ponen en jaque elementos fundantes del sistema de protección de datos"* (p.19). En consecuencia, diversos países a nivel global destacan la importancia de fomentar regulaciones e incorporar la anonimización de datos en sus marcos normativos. En este contexto, resulta imperativo llevar a cabo un análisis comparativo de las normativas vigentes en Ecuador y México.

Para garantizar el derecho a la protección de datos personales, se establecieron los fundamentos principales para regular los aspectos más importantes en esta materia. En consecuencia, se promulgó la Ley Orgánica de Protección de Datos Personales (2021), la cual en su artículo 4 define la anonimización como "*la aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados*" (Asamblea Nacional del Ecuador, 2021, art. 4). Asimismo, el artículo 37 ibidem, establece la anonimización como una medida esencial de seguridad de datos personales.

Según Lasso Roldán (2024) la implementación de la anonimización presenta beneficios significativos, como la reducción de violaciones a la privacidad al minimizar la posibilidad de identificación de los datos

almacenados. Además, facilita las investigaciones y el cumplimiento de regulaciones normadas en ley. En este sentido, tomando sus palabras y dando el sentido a la protección de la información de los titulares, promueve el empleo de manera segura, confiable y ética de aquellos datos personales que son tratados con fines de investigación y análisis, o en el caso de las empresas con la finalidad de dar cumplimiento a la LOPD y evitar sanciones ocasionadas por su incumplimiento

En el contexto mexicano, esta práctica establecida como disociación de datos personales está regulada primordialmente por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), misma que constituye el marco legal nacional en materia de protección de datos. De acuerdo con el artículo 19 de la LFPDPPP, los responsables del tratamiento de datos personales tienen la responsabilidad de implementar medidas de seguridad administrativas, técnicas que permitan proteger los datos personales contra daño, alteración, destrucción o el uso o acceso no autorizado (Cámara de Diputados del Honorable Consejo de la Unión, 2010).

La anonimización es reconocida como una medida de seguridad fundamental que puede ser implementada en la gestión de datos personales con el objetivo de salvaguardar la privacidad de los individuos. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México (INAI), entidad encargada de supervisar el cumplimiento de la LFPDPPP, define la anonimización de datos como una práctica que permite convertir los datos de tal forma que no es posible identificar a los titulares de estos. Es una técnica que posibilita reducir los riesgos que se presentan en la obtención y tratamiento masivo de datos personales.

Entonces, la anonimización de datos desempeña un papel fundamental en la preservación de la privacidad, asegurando que la información sensible esté resguardada y fuera del alcance de terceros no autorizados. Mediante la transformación de los datos en una forma irreconocible, se salvaguarda y

preserva la confidencialidad de la información sin menoscabar su utilidad para propósitos legítimos, como la investigación científica.

En un contexto donde la recolección y el análisis de datos son pilares fundamentales para el funcionamiento de diversas organización y sistemas, la técnica de anonimización ha adquirido una creciente relevancia. Al aplicar rigurosos estándares para ello, las instituciones pueden mitigar los riesgos inherentes al acceso no autorizado o al uso erróneo de la información personal. Este enfoque no solo fomenta la confianza y la transparencia en la gestión de datos, sino que también fortalece los principios éticos y legales que rigen la protección de la privacidad en el ámbito digital.

En conclusión, la anonimización de datos emerge como un paso esencial en la defensa de la privacidad en la era digital. Al integrar esta práctica como un estándar en el tratamiento de datos personales, se fortalecen los fundamentos de transparencia y responsabilidad en la sociedad. Este enfoque promueve un entorno propicio para el uso seguro y ético de la información, asegurando el cumplimiento de las normativas legales y la protección de los derechos individuales en el ámbito digital.

Al hablar de la anonimización, debemos también referirnos sobre a seudonimización; en este sentido, la Ley Orgánica de Protección de Datos Personales de 2021 establece una forma de tratamiento para deslindar al titular de datos personales de la información generada en determinada base de datos, pero manteniendo la posibilidad de usar información adicional para identificarlo, este proceso se denomina como seudonimización y la normativa citada la ha definido como:

> Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. (Asamblea Nacional

> del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021, art. 4 inc. 20)

La ley ecuatoriana lo ha colocado como el tratamiento de separar a la información y los datos personales generando dos bases de datos distintas que solo pueden volver a individualizar al titular cuando se combinan, lo que implica la posibilidad de re identificar, por lo tanto, esta medida de seguridad tiene la necesidad de usar dos encargados de datos personales dentro del mismo organismo o equipos separados para manejar las bases de datos pero bajo la dirección de un mismo responsable y por ende con fines iguales. La seudonimización bajo un argumento *ad-rúbrica* del capítulo VI de la Ley Orgánica de Protección de Datos Personales y su artículo 37 establecen a esta forma de tratamiento como una medida de seguridad a fin de garantizar confidencialidad o en el caso de usuarios financieros el sigilo bancario cuando se usa la información para fines estadísticos.

La legislación del parlamento europeo ha definido a la seudonimización en el Reglamento (EU) 2016/679 de 27 de abril de 2016, en su artículo 4 numeral 5 que establece que:

> 5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. (Parlamento Europeo y el Consejo de la Unión Europea, Reglamento (EU) 2016/679, 2016, art. 4 núm. 5)

En este caso se define a la seudonimización como una forma de tratamiento que impide la identificación del titular sin información adicional, similar a la definición ecuatoriana requiere manejar la información por separado, pero el Reglamento (UE) 2016/679 de 27 de abril de 2016 da mayores características a la seudonimización, en su considerando 26 menciona que los datos seudonimizados son para personas físicas

identificables (Parlamento Europeo y el Consejo de la Unión Europea, 2016). Lo que implica la adición de términos como datos personales seudonimizados que de forma razonable permiten identificación del titular y la característica de que son datos personales para titulares identificables, por lo tanto, no permiten dar una confidencialidad total al sujeto de derechos, también al ser datos personales identificables mantienen la protección que otorga la legislación a los datos personales, distinto a lo que sucede con datos personales anonimizados que ya no generan un vínculo con el titular y no están sujetos a la legislación.

La legislación española aplicando las directrices del Reglamento (UE) 2016/679, expidió la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales de 5 de diciembre de 2018, pero en esta norma el enfoque de la seudonimización está dirigida al sector de la salud e investigación médica mediante disposiciones adicionales, establece directrices acordes a la definición del artículo 4 del Reglamento (UE) 2016/679, la ley española en su disposición adicional decimoséptima dispone que en investigaciones médicas es licito el uso de datos seudonimizados pero deberá existir una separación funcional entre el equipo investigador y el equipo que maneja los datos, es decir se crea dos encargados de datos con fines distintos (Jefatura del Estado de España, 2018). Pero es importante señalar que se determina la licitud del uso de estos datos, aunque sean de personas identificables aun sujetas a protección.

Por otro lado, si bien no muchas legislaciones manejan el tema de la seudonimización, en Estados Unidos el estado de California expidió la *California Consumer Privacy Act* en 2018 como parte del Código Civil, esta norma plantea obligaciones para proteger a los consumidores en el manejo de sus datos como forma de garantizar la privacidad, en la disposición 1798.140. literal (aa) se explica que la seudonimización implica que la información personal del consumidor ya no puede atribuirse a su titular sin información adicional, por lo tanto, la información debe estar dividida. Al igual

que la legislación española, ecuatoriana y europea, se solicita la existencia de bases de datos separadas, también es posible la identificación del titular, pero esta norma estadounidense está enfocada en protección de consumidores, aunque emplea una definición restringida a determinados sujetos de derechos cumple los mismos propósitos del resto de legislaciones analizadas.

En el análisis comparado se puede observar una similitud en las definiciones propuestas a la seudonimización en las legislaciones usadas, es decir se le otorga contenido como la forma de tratamiento que implica separar la información almacenada y los datos personales del titular, por ejemplo, si el ciudadano con número de ciudadanía establecido debe quinientos dólares deberán separarse los datos personales de la información crediticia creando dos bases de datos distintas, una que mantenga el nombre del deudor y otra con un código seudónimo que exponga su información crediticia.

En las legislaciones se contempla, de forma explícita en la europea, o tácita en el resto, que los datos personales seudonimizados son de titulares identificables porque no se rompe la relación causal entre la información y la persona natural, porque mediante procedimientos razonables puede individualizarse al sujeto de derechos, es decir estos datos son objeto de protección, además la información seudonimizada mantiene un carácter menos rígido que la anonimizada, la facilidad de recuperación eleva el riesgo de identificación y por lo tanto requiere mayor diligencia del encargado y el responsable. Si bien todas las legislaciones contemplan la separación funcional y técnica solo la española interpreta que existirán dos encargados de tratamiento, el resto lo deja implícito, como la ecuatoriana donde queda la posibilidad de emplear dos encargados o equipos dentro de una misma organización.

Capítulo III

1.3. Proceso que aplican las instituciones bancarias, para el ejercicio de la anonimización o bloqueo de datos personales de sus clientes

Resulta trascendental traer a colación ciertas particularidades que distinguen al sector financiero del resto de industrias en el país, dada la permanente, rigurosa y excesiva regulación normativa en la materia, evidencia de ello encontramos en el actual Código Orgánico Monetario y Financiero (2014), con las disposiciones sobre sigilo y reserva bancaria del artículo 353, así como la obligatoriedad de archivo de la información por 10 años cuando estén en formato físico, y 15 años respecto respaldos en formato digital, conforme el artículo 225 *ibidem* (Asamblea Nacional del Ecuador, 2014). En este sentido, encontramos similares sustentos que pretenden consolidar el derecho constitucional a la protección de datos personales, sumada a la acción constitucional de Habeas Data, como mecanismo de ejercicio del derecho al acceso y eliminación de dicha información, en los supuestos que la misma Constitución lo determina.

Dado que la Ley Orgánica de Protección de Datos Personales define al dato personal con su categorización y enunciación de derechos inherentes a los titulares, es importante centrarnos en la eliminación, bloqueo o anonimización, encasillando las circunstancias que le permitan ejercerlo, y con ello arribar en los datos tratados crediticios que son de interés de las entidades bancarias; es así que, esta norma los define como "*aquellos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera*" (Asamblea Nacional del Ecuador, Ley de Protección de Datos Personales, 2021, artículo 4).

A efectos de la actividad económica de las instituciones bancarias, los datos aquí descritos tienen por objeto informar sobre la solvencia patrimonial o crediticia, incluyendo aquellos relacionados al cumplimiento de obligaciones contractuales. Con ello se comprenden como tal las conductas comerciales o capacidad de endeudamiento del titular de los datos, sea que se recopilen por fuentes de acceso público o procedentes del mismo titular, así como por terceros legítimamente autorizados para el efecto.

En este punto, es preciso traer a colación normativa comparada, en específico la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales de España, referente para la redacción de la normativa ecuatoriana en la materia pues, define a la información crediticia en iguales condiciones, aunque con enfoque con tendencia a cartera vencida. En este sentido, la parte pertinente de su texto señala "*Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes*" (Jefatura del Estado de España, Ley Orgánica 3/2018, 2018, art. 20); además, que dichos datos se mantengan solo mientras el incumplimiento persista, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

Dada la regulación normativa al sector financiero, y puntualmente de las instituciones bancarias del sector privado, encontramos ciertas interpretaciones normativas respecto el ejercicio del derecho a la eliminación de datos personales; entre ellas, la disposición del artículo 225 de Código Orgánico Monetario y Financiero, sobre la necesidad de que los respaldos contables sean custodiados, resguardados y protegidos; a efectos de los requerimientos dispuestos por los organismos de supervisión, así como la prestación optima de productos y servicios financieros de manera constante e ininterrumpida (Asamblea Nacional del Ecuador, 2014). Es aquí cuando nos enfocamos a los bancos privados y su necesidad de implementar mecanismos o técnicas de bloqueo o anonimización de datos, como una alternativa efectiva que coadyuve a mantener la seguridad de legítimo uso determinado por el artículo 7 de la LOPDP, precautelando por tanto la prestación de los productos y servicios financieros que son de orden público por definición.

Luego de comprender el entorno normativo aplicable a las entidades bancarias del Ecuador, es oportuno aterrizar al tratamiento de datos de sus

consumidores financieros, y en virtud de ello comprender los casos en los que procede la anonimización y bloqueo de dicha información.

En esta línea, y dado que las actividades financieras son un servicio de orden público por disposición expresa de la Constitución de la República del Ecuador (2008, art. 308), las entidades bancarias son controladas por la Superintendencia de Bancos, entidad del estado encargada de la "*vigilancia, auditoría, intervención, control y supervisión de las actividades financieras que ejercen las entidades públicas y privadas del Sistema Financiero Nacional, así como de autorizar mediante resolución administrativa el funcionamiento de las entidades financieras sujetas a su supervisión*" (Asamblea Nacional del Ecuador, Código Orgánico Monetario y Financiero, 2014, art. 60), y dentro de dichas facultades está la de conceder el permiso para la oferta y prestación de productos o servicios financieros según el numeral 2 del artículo 62 *Ibidem*, segmentado entre actividades activas, pasivas, contingentes y de servicios.

Este órgano de supervisión, además de las funciones arriba destacadas, es el encargado de emitir normativa de carácter técnico y administrativo, que permita garantizar el antedicho servicio de orden público, para lo cual, exige a las entidades financieras contar con estructuras organizativas adecuadas, así como manuales, procesos, protocolos y procedimientos oportunos que protejan al consumidor financiero, garantizando con ello la continuidad de la prestación de dichos servicios.

Parte de estos requerimientos los encontramos en la Norma de control para la gestión del riesgo operativo, contenida dentro de la Codificación de resoluciones de la Superintendencia de Bancos, Libro Primero, Tomo II, dentro del cual exige a las entidades controladas mantener procedimientos que permitan la adecuada gestión del riesgo en el desenvolvimiento de sus actividades financieras; resaltando la gestión de Seguridad de la Información en la finalidad de salvaguardar la información que repose en la entidad financiera (Superintendencia de Bancos, Resolución 810, 2017, arts.. 24 - 26).

Con ello, las entidades bancarias han venido desarrollando mecanismos que garanticen la confidencialidad, sigilo y reserva de la información de sus clientes, lo cual resulta un punto de partida para complementar la protección de información financiera que, si bien son procedimientos simétricos, si guardan conexiones directas al proteger la información que consta en sus repositorios.

En el desarrollo de esta investigación, y con el análisis a los procesos realizados por una de las entidades bancarias del sistema financiero nacional (cuyo nombre no pueden ser expuestos por la confidencialidad que esta ha requerido se mantenga), hemos encontrado tendencias o patrones similares, en cuanto refiere a la anonimización de datos personales. En estos procesos es importante delimitar un proceso concatenado, que va desde las finalidades de la anonimización (sin que se contemple como una causa de este proceso al requerimiento del cliente), así como el proceso que siguen para llevarlo a cabo. Las entidades financieras aplican métodos de disociación o encriptación en varias actividades de tratamiento, tales como:

1. Análisis estadístico relacionado con tendencias de usabilidad en canales digitales y presenciales, patrones de consumo de sus clientes, niveles y volumen de transaccionalidad, entre otras métricas vinculadas a estas finalidades.
2. Elaboración de modelos de riesgo, que permitan evaluar tanto la capacidad de pago o solvencia crediticia, como fuentes de repago, y en virtud de aquello ofrecer productos o servicios financieros ajustados a sus necesidades. Aunque en una finalidad subsecuente, dichos modelos de riesgo también tienen por objeto cumplir con la normativa relacionada a la prevención de lavado de activos, protegiendo la privacidad de sus clientes, conforme lo señala el artículo 12 y siguientes de la Norma para las entidades de los sectores financieros público y privado sobre prevención de lavado de activos, y del financiamiento de delitos como el terrorismo (Superintendencia de Bancos, Resolución SB-2024-0316, 2024).

3. Investigaciones académicas para el desarrollo y crecimiento el sector financiero, relacionadas con educación financiera, inclusión al mercado financiero de grupos prioritarios mediante la creación de productos adecuados a su perfil; y en definitiva consolidación de la responsabilidad social empresarial. Estas investigaciones o estudios pueden ser asimismo publicados, respetando siempre la privacidad y anonimización de datos de sus clientes.
4. Cumplimiento normativo, cuya finalidad sea consolidar la garantía de derechos de los clientes de la entidad financiera respecto la protección de sus datos personales, en especial la oposición, eliminación y suspensión del tratamiento, cuando exista la correspondiente justificación jurídica.
5. Análisis del comportamiento de los clientes, sus preferencias de para mejorar la experiencia del usuario y los servicios ofrecidos, el banco puede utilizar datos anonimizados para evitar revelar información personal.
6. Transferencia de datos a terceros, sea que estos estén domiciliados en el país o en el exterior, en finalidades directamente relacionadas con la prestación de productos y servicios financieros, entre las que se pueden enunciar marketing, publicidad o afines, protegiendo la privacidad de sus clientes, en términos de confidencialidad, sigilo y reserva bancaria.

Según la LOPDP, los responsables del tratamiento de datos personales deben informar al titular, entre otros aspectos, las finalidades del tratamiento, base legal y tipos de tratamiento de sus datos, evidencia en las políticas de protección de datos que, para las entidades financieras, constan publicadas en sus portales web institucionales (Asamblea Nacional del Ecuador, 2021, art. 12).

Según señala la Guía básica de anonimización, elaborada por la Asociación Española de protección de datos, hay una diferencia sustancial entre la definición de anonimización y desidentificación, pues la primera se considera como "*la conversión de datos personales en datos que no se pueden utilizar para identificar a ningún individuo*" (Agencia Española de

Protección de Datos, 2022, p. 6), mientras que la desidentificación refiere a la eliminación de datos que puedan hacer identificable a una persona natural (Agencia Española de Protección de Datos, 2022). Y aunque el documento comenta que suelen confundirse ambos términos como anonimización, lo cierto es que en la realidad ecuatoriana la confusión sucede también con el término disociación, que dentro de las definiciones precisas se concibe como "*El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo*" (Cámara de Diputados del Honorable Consejo de la Unión, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010, art. 3 núm. VIII).

Con este entorno, es importante diseñar un procedimiento metódico y razonable para la correcta aplicación de la anonimización de datos personales de los consumidores financiero; por cuanto, lo pertinente es atender y replicar ciertos de los lineamientos que determine la AEPD, así como los lineamientos que al respecto determina el GDPR.

Tomando en consideración las prácticas adoptadas por la entidad financiera de la cual se ha basado esta investigación, resulta primordial el trabajo conjunto de las diversas unidades que se dediquen a la administración y gestión de la data, así como seguridad de la información, servicios tecnológicos, asesoría jurídica, y la constante supervisión del delegado de protección de datos; a efectos de determinar un procedimiento pormenorizado y flexible. Dicho procedimiento se utiliza en específico para aquellos casos en los cuales no existe la solicitud expresa del consumidor financiero para eliminar, anonimizar o bloquear, por lo que se enmarca en los siguientes lineamientos:

a) Definir el objetivo de la disociación, puntualizando tipos y categorías de datos que serán tratados para este fin, su motivación, razonabilidad y justificación. En este proceso se debe tomar especial atención a la identificación de datos sensibles que serán objeto del tratamiento.

b) Definición de la técnica de anonimización a aplicarse según el tipo de requerimiento de anonimización.
c) Determinación de responsables para la administración de la anonimización según su finalidad.
d) Ejecución de anonimización en el ciclo de vida del dato, tanto en las pruebas como en la integridad del entregable, para asegurar su disociación en los casos que requieran su destrucción, así como la recuperación mediante llaves o permisos únicos en aquellos casos en los que el tratamiento de datos siga siendo necesario para cumplir con la prestación de servicios o productos financieros.
e) Supervisión del cumplimiento de la anonimización por parte del delegado de protección de datos junto con el área de auditoría interna, tanto del proceso implementado como de la norma vigente aplicable. Esta supervisión es extensiva a la necesidad de modificación o actualización de los procesos establecidos para el efecto.
f) Capacitación a los colaboradores de la organización en general, tanto en el tratamiento de datos personales, y de manera puntual a los dueños de los dominios de datos, en cuanto la importancia de la anonimización, a través del entrenamiento continuo.

Capítulo IV

1.4. Regulación del bloqueo o anonimización de datos personales frente al derecho de eliminación de los consumidores bancarios.

La Ley Orgánica de Protección de Datos Personales en su artículo 15 prevé un procedimiento para la eliminación, bloqueo o anonimización de datos personales que inicia con la solicitud del titular o representante legal, el mismo artículo establece que el Responsable será el competente para responder la solicitud y otorga un plazo de 15 días desde que recibe la solicitud para responder ya sea con negativa o aceptación (Asamblea Nacional del Ecuador, 2021), en este caso la ley no establece un procedimiento para ejercer el derecho de eliminación sino crea una forma de iniciar el mismo, es decir

transfiere el “impulso” al titular, el mismo artículo 15 inciso final ibidem menciona que el procedimiento de para eliminar, hacer ilegible o dejar irreconocibles los datos personales son responsabilidad del Responsable del tratamiento, es decir otorga libertad de implementación de los métodos y técnicas, pero no hay en la ley definido un procedimiento específico. Es decir, la ley mencionada regula la petición del derecho de eliminación, por lo tanto, solo el inicio del procedimiento.

La Ley establece ciertas pautas para entender el procedimiento a seguir previo a la eliminación de datos personales, ya sea con la petición del interesado o casos específicos como en la aplicación del derecho a la portabilidad del artículo 17 donde su inciso segundo establece que *“…Luego de completada la transferencia de datos, el responsable que lo haga procederá a su eliminación, salvo que el titular disponga su conservación…*” (Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales, 2021, art. 17), es decir cuando existe transferencia de datos de un responsable a otro por solicitud del interesado, si el titular ordenará la eliminación se procederá con la misma salvo exista una excepción o tratamiento legítimo como los establecidos en el artículo 7 y 18 de la Ley Orgánica de Protección de Datos Personales, en ese caso el Responsable podrá decidir si inicia un tratamiento de bloqueo o anonimización como medida sustituta.

El artículo 29 numeral 3 de la Ley Orgánica de Protección de Datos Personales establece algunas especificaciones para el ejercicio de derechos sobre datos personales cuando son datos crediticios, entre ellos prevé que pueden dirigirse solicitudes también a las fuentes de información mediante solicitud escrita, en este caso ya no solo es el responsable el ente competente para conocer solicitudes sino cualquier fuente de información sobre datos crediticios (Asamblea Nacional del Ecuador, 2021), por ejemplo para que el titular elimine sus datos del buró de crédito cuando ha cumplido con sus obligaciones. De igual forma se otorga 15 días para responder la solicitud

motivando su decisión, es decir sea pública o privada se ha impuesto la obligación de justificar. Cualquier derecho que se solicite a los prestadores de servicios también, en conjunto, se puede pedir se señale en los reportes que comunican que la información está en revisión, lo cual, en caso de aprobarse de eliminación, por ejemplo, sería un paso previo, pero a solicitud del interesado (Asamblea Nacional del Ecuador, 2021).

El artículo 62 de la Ley Orgánica de Protección de Datos Personales establece que el requerimiento de eliminación ante el responsable realizado por el titular es del tipo de directo, el mismo será gratuito y sumario o sencillo para que la persona natural pueda realizar cualquier solicitud, queja, reclamo o peticiones y recibe respuesta en 15 días (Asamblea Nacional del Ecuador, 2021). Sin embargo, el inciso 2 ibidem establece un término de 10 días para contestar, notificar y ejecutar lo que corresponda, en este caso es una norma general que establece un término para actuaciones no específicas, porque para responder a la solicitud de eliminación existe 15 días plazo, pero quedará posiblemente a análisis de la Autoridad de Protección de Datos Personales si el plazo de respuesta es de 15 días plazo y la notificación y ejecución de la respuesta deberá realizarse en 10 días término, por el lenguaje establecido deberá interpretarse de forma sistemática el Código Orgánico Administrativo o el Código Orgánico General de Procesos para diferenciar plazos y términos. La misma norma en el artículo 65 ibidem establece que cuando exista medidas correctivas también podrá procederse a la eliminación de datos personales según el inciso 2 numeral 2 del citado artículo (Asamblea Nacional del Ecuador, LOPDP, 2021), lo que implica que la Autoridad en consecuencia de un procedimiento administrativo puede eliminar de forma forzosa datos personales, esto según lo establecido en el artículo 16 del Reglamento de aplicación general a la Ley Orgánica de Protección de Datos Personales cuando no exista respuesta oportuna o el titular crea vulnerados sus derechos (Presidencia de la República del Ecuador, 2023) o por inicio de procedimientos sancionatorios de oficio.

El Reglamento de aplicación general a la Ley Orgánica de Protección de Datos Personales (Presidencia de la República del Ecuador, 2023) establece en su artículo 12 que la recepción de solicitudes o cualquier requerimiento será fácil y gratuito permitiendo el uso de plataformas físicas o digitales, es decir cualquier medio de comunicación sería idóneo para realizar la solicitud siempre que se demuestre la calidad en que se comparece. El artículo 13 del Reglamento establece que la solicitud debe contener las generales de ley del titular, la identificación del dato personal sobre el que se requerirá un derecho o forma de localización, la pretensión, el derecho que se quiere ejercer y los documentos habilitantes. Ante cualquier solicitud y en caso de requerirse información adicional el responsable tiene, según el artículo 14 del Reglamento, la potestad de solicitar correcciones dentro de 5 días término de recibida la solicitud, y el titular contará con 10 días para aclarar bajo pena de archivo de la solicitud, sin perjuicio de poder presentar otra igual. Los responsables tienen la obligación según el artículo 15 ibidem de registrar todas las solicitudes.

Una cuestión que incorpora el artículo 64 de la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021) es la vía administrativa para exigir los derechos como el de eliminación, principalmente la remisión al Código Orgánico Administrativo para seguir las reglas generales del procedimiento administrativo, lo que implica que se podrá aplicar el silencio administrativo, un término de prueba de hasta 30 días u oralidad a petición de la Autoridad (Asamblea Nacional del Ecuador, 2017), es decir la normativa ecuatoriana no prevé un procedimiento especial para gestionar un procedimiento administrativo ante la Autoridad sino que permite usar las reglas generales del Código Orgánico Administrativo y las previstas por el Superintendente de Datos Personales, contemplando la garantía del debido proceso constitucional del artículo 76 de la Carta Magna y el inciso final del artículo 16 del Reglamento de la Ley Orgánica de Protección de Datos Personales que determina que en los procedimiento de reclamos previstos ante la Autoridad exista un derecho a la defensa para el Responsable.

Analizada la legislación ecuatoriana se requiere hacer un análisis comparado con la normativa mexicana, en este caso la Ley Federal de Protección de Datos Personales en Posesión de Particulares (Cámara de Diputados del Honorable Consejo de la Unión, 2010) establece que el titular de derechos podrá iniciar una solicitud para ejercer el derecho de acceso, rectificación, cancelación u oposición contra el responsable según el artículo 29 de la mencionada Ley, respecto al contenido de la solicitud la información requerida es similar a la ecuatoriana, excepto que el artículo 29 de la ley mexicana exige entregar cualquier elemento o documento que facilite la localización, contrario a Ecuador que solicita de ser necesario solo una descripción. En el caso de los plazos de respuesta el artículo 32 permite que el responsable responda en máximo 20 días con plazo prorrogable por una sola vez según el mismo artículo en su inciso final, pero con una motivación del responsable. Respecto al derecho de cancelación que es similar al de eliminación en Ecuador, México establece en su artículo 32 de la Ley Federal de Protección de Datos Personales en posesión de Particulares y 107 del Reglamento de aplicación de la mencionada ley, que en el plazo de veinte día deberá comunicarse del plazo de bloqueo de forma motivada y desde la respuesta a la solicitud de ser favorable, existe un plazo de 15 días para bloquear los datos por el tiempo determinado en la respuesta a la solicitud (Cámara de Diputados del Honorable Consejo de la Unión, 2010; Presidencia de los Estados Unidos Mexicanos, 2011).

Continuando con lo anterior, esto solo referente a lo que sería una solicitud directa del interesado, pero en caso de existir controversias o el titular establezca que se han vulnerado sus derechos puede acudir ante la autoridad que es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México (INAI) según el artículo 38 de la norma mexicana, esta tiene un plazo de 50 días para resolver según el 47 de la ley federal con posibilidad de prórroga, pero en el devenir de ese periodo existe otros tiempos como los mencionados en el artículo 45 inciso 4 ibidem que da un plazo de 15 días desde recibida la solicitud para que el responsable

ejerza una defensa, pero previo a esto, desde recibida la solicitud el Instituto tiene hasta 10 días para calificar la solicitud y otros diez para correr traslado al Responsable de Datos Personales, según el artículo 117 del Reglamento (Cámara de Diputados del Honorable Consejo de la Unión, 2010; Presidencia de los Estados Unidos Mexicanos, 2011). Cumplidos los primeros términos o/y plazos, en el tiempo restante previo a cumplir los 50 días o el doble de tiempo si se hubiera aumentado, el artículo 118 del reglamento de la ley federal establece un tiempo de presentación de pruebas y de acuerdos probatorios, así como una audiencia donde existe comparecencia, a diferencia de Ecuador donde por disposición del artículo 137 del Código Orgánico Administrativo la audiencia está condicionada y puede ser a discrecionalidad del órgano administrativo, mientras el periodo de prueba no puede exceder de 30 días según el artículo 194 inciso 4 ibidem (Asamblea Nacional del Ecuador, 2017). Por disposición de la ley federal el Instituto en México habilita la conciliación en la sustanciación del procedimiento administrativo después del auto de admisión de pruebas, durante 10 días se puede manifestar la voluntad de conciliar (Cámara de Diputados del Honorable Consejo de la Unión, 2010). Caso contrario se llamará a audiencia y se emitirá resolución.

Si bien la legislación mexicana prevé un procedimiento especial en vía administrativa, a diferencia de Ecuador que recurre a su norma supletoria creando un procedimiento general que puede ser aplicado de forma especial mediante resoluciones de la Autoridad de Datos Personales, se puede establecer pautas por otras normas supletorias y crear un procedimiento especializado como el de México, por ejemplo el reconocimiento de medios alternativos de solución de conflictos esta especificado en el artículo 190 de la Constitución de la República del Ecuador, y esta es de aplicación directa (Asamblea Constituyente, 2008). En México se ha dado ciertas pautas para dar facilidades a los responsables, por ejemplo, la capacidad de ampliar términos o plazos en la solicitud directa cuestión que Ecuador no regula, pero la legislación ecuatoriana permite que se aplique el silencio administrativo por disposición del artículo 207 del Código Orgánico Administrativo para

solicitudes que no se tramiten cuando se dirige el reclamo por falta de respuesta ante la autoridad administrativa en 30 días término (Asamblea Nacional, 2017), una figura que de forma expresa no analiza la ley y reglamento de México.

Para tomar otra normativa, el caso de España establece la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales que es consecuencia del Reglamento (UE) 2016/679 de la Unión Europea, por eso debe analizarse en su conjunto. Para los casos de solicitud directa al ejercicio del derecho de supresión que es el homologo a la eliminación en Ecuador y cancelación en México, Europa y España prevé mediante el Reglamento (UE) 2016/679, en su artículo 14, un periodo de un mes prorrogable a dos para responder solicitudes de los titulares para el ejercicio de derechos como el de supresión (Parlamento Europeo y el Consejo de la Unión Europea, 2016), sin embrago al igual que México, España mediante su ley orgánica introduce el paso previo a la supresión usando el bloqueo, ya que en su artículo 32 numeral 1 establece que deberá cumplir con esa obligación cuando proceda a la supresión (Jefatura del Estado de España, 2018), pero igual que México establece que el Responsable podrá motivar el tiempo de bloqueo. A diferencia de Ecuador o México que permitían solo al titular o su representante dirigir solicitudes al Responsable, España en su artículo 12 de la Ley Orgánica 3/2018 agrega la figura del voluntario, por lo tanto, cualquiera puede ejercer derechos sobre datos personales a nombre de un tercero, el mismo artículo permite al encargado de datos personales tener competencia para tramitar solicitudes cuando su contrato lo permita, mientras que en las demás legislaciones analizadas solo el responsable es competente para receptar y tramitar; una cuestión importante en la ley española es el artículo 12 numeral 4 ibidem que crea una reversión de la carga de la prueba donde el Responsable debe probar el cumplimiento de sus obligaciones (Jefatura del Estado de España, Ley Orgánica 3/2018, 2018), distinto a Ecuador o México donde debe usarse la regla general del Derecho que establece que la carga de la prueba recae sobre el que alega, solo en España

el responsable debe justificar con evidencia mientras en el resto de legislaciones es suficiente una motivación escrita. España al igual que México y Ecuador reconoce la gratuidad de estos procedimientos y su facilidad.

Analizado el procedimiento de solicitud directa en España en concordancia con el Reglamento de la Unión Europea, se resalta que aparte de la solicitud directa, el artículo 37 de la Ley Orgánica 3/2018 de España permite que el afectado por una violación a la mencionada Ley o el Reglamento (UE) pueda dirigir reclamos o solicitudes ante el delegado de protección de datos personales de la entidad contra la que actúe, dando un tiempo de resolución al Delegado de 2 meses para resolver, así mismo el artículo 37 numeral 2 ibidem permite a la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos redirigir reclamos sobre una entidad a su delegado (Jefatura del Estado de España, 2018). Es decir, para solicitar el bloqueo y supresión de datos en caso de negativa de la entidad puede remitirse solicitud al delegado, y con posterioridad a los órganos de control españoles. También el artículo 65 numeral 4 inciso 2 de la ley española permite que la redirección de la reclamación por posibles derechos como el de supresión sean dirigidos ante el encargado de datos en ausencia del delegado.

En España existe un procedimiento de solicitud directa, solicitud ante el delegado y un procedimiento administrativo donde actúan los órganos de control para protección de datos personales, el artículo 64 numeral 1 de la Ley Orgánica 3/2018 menciona que ante la falta de atención a derechos como el de supresión del artículo 17 del Reglamento (UE) 2016/679, podrá dirigirse petición a la Agencia Española de Protección de Datos que deberá resolver en seis meses desde la recepción de la solicitud ante negativas de los responsables y encargados cuando el titular quiere suprimir sus datos, pero de forma expresa, caso contrario a Ecuador que lo establece con la remisión a su norma en materia administrativa, le ley española reconoce el silencio administrativo positivo, según el inciso 2 del numeral 1 del artículo 64 de la

Ley Orgánica 3/2018, cuando determina que el interesado considerará estimada su solicitud si no hay resolución en 2 meses. A diferencia del resto de legislaciones analizadas, España prevé que el artículo señalado sea exclusivo para solicitudes de derechos como el de supresión rechazados sin perjuicio de inicio de procedimientos sancionatorios donde se apliquen medidas correctivas que dispongan la eliminación por vulneración de derechos.

Un dato importante de las reclamaciones ante la Agencia Española de Protección de Datos Personales es que según el artículo 65 inciso 1 de la Ley Orgánica 3/2018 (Jefatura del Estado de España,2018) puede desestimar las reclamaciones por falta de evidencia, a diferencia de la solicitud directa donde el responsable debe probar cumplir de forma diligente y lícita su trabajo, ante las Autoridades de control de España la carga de la prueba es del interesado, distinto a Ecuador donde según su Código Orgánico Administrativo deben probarse los hechos controvertidos y en caso de procedimientos sancionadores la carga de la prueba recae sobre la administración pública según el artículo 194 del mencionado código (Asamblea Nacional del Ecuador, 2017), esto implica que a diferencia de Ecuador, España obliga a los titulares a probar cada hecho del que se vean asistidos sea controvertido o no así como tener la capacidad de poder proporcionarlos, esto implica una situación de desventaja cuando una persona natural como titular busca enfrentarse ante un persona jurídica que actúa como responsable y tiene mayores recursos que el interesado. Si bien ciertas normas analizadas de España son sobre reclamos, es importante señalar que los interesados pueden acudir ante los órganos competentes en forma de queja cuando sus solicitudes son rechazadas, aunque de forma exclusiva la ley española ya establece un procedimiento cuando se trata de rechazo de solicitudes con un plazo sujeto a silencio administrativo positivo.

Si bien el procedimiento administrativo también está previsto en las legislaciones analizadas como un mecanismo para obtener del responsable la

eliminación, cancelación o supresión de datos personales, este análisis está delimitado solo a las solicitudes porque las competencias sancionadoras de los órganos administrativos pueden extenderse por encima de reclamaciones por negativas hacia solicitudes de los titulares. En las legislaciones analizadas se establece que solo la española y la mexicana prevén un procedimiento administrativo especial para que el interesado obtenga la eliminación de sus datos, pero en conjunto las tres determinan la solicitud directa del titular, pero pueden variar quien es el competente para resolver cuando no va dirigida a la autoridad administrativa, como España que los delegados y encargados pueden resolver sobre las solicitudes pero en el resto de normativas no, además respecto a los términos y plazos solo Ecuador no autoriza los aplazamientos. Todas la legislaciones contemplan el principio de gratuidad y la facilidad para los titulares de dirigir solicitudes para eliminar sus datos personales, pero solo España y México establecen la posibilidad de borrar las bases de datos aunque deba pasar el tiempo de bloqueo, mientras en Ecuador salvo norma especial como es el caso del Código Orgánico Monetario y Financiero Libro I que prevé la eliminación de datos crediticios después de 15 años de conservación en fuentes digitales, no se establece al bloqueo como una medida previa sino como una actuación sustitutiva, es decir está dirigida a datos específicos mientras en España y México son una regla general.

Para aplicar los derechos de los consumidores bancarios, en cuanto a protección de datos, las instituciones financieras deben aplicar el derecho de eliminación, siendo el titular el responsable del tratamiento de datos personales de cada entidad conforme establece el último inciso del artículo 15 (Asamblea Nacional del Ecuador, LOPDP, 2021). Sin embargo, con la expedición del Reglamento a la Ley, se deduce que el procedimiento que los titulares deben seguir para ejercer cualquiera de los derechos a ellos inherentes como el de actualización, rectificación o eliminación, son los siguientes:

1. La solicitud solo la presentará el titular del dato. Aquí es vital referirse al mandato como institución jurídica del derecho civil, toda vez que podría presentarlo también quien tenga la facultad legal de representar al interesado o consumidor afectado.
2. Deberá presentar su solicitud ante la institución financiera de la cual es cliente o consumidor, sea a través de agencias físicas o los demás canales que para tal efecto determine el responsable.
3. La solicitud deberá ser de manera escrita.
4. La entidad financiera, dentro del término de diez días de presentada la solicitud, deberán resolverla admitiéndola o rechazándola motivadamente.
5. Si el responsable de la información requiere aclarar o ampliar la solicitud, podrá requerir al titular, por una sola vez y en cinco días de recibida la solicitud, que la aclare o complete.
6. El recurrente tendrá el término de diez (10) días contados a partir del día siguiente a la notificación, para aclarar o completar la solicitud.

Aunque la normativa citada establece las formalidades aplicables al caso, estas deberán perfeccionarse por la Autoridad de Protección de Datos, cumpliendo el principio de celeridad e informalidad en todo lo posible; por ello, es trascendental comprender el rol de control y regulación que implementará la autoridad de protección de datos; para no contraponer su normativa con la ya plenamente implementada en materia de regulación bancaria. Tal es así que, la norma antes aludida ya especifica disposiciones de carácter mandatorio y de obligatorio cumplimiento de las entidades financieras controladas, pues el numeral iv) del mismo literal y articulo, especifica la obligación de precautelar los datos no públicos de los consumidores financieros y en especial la necesidad de que puedan ser corregidos, completados, destruidos o limitados, según sea pertinente.

Para que el consumidor bancario pueda acceder a los derechos consagrados por la Ley Orgánica de Protección de Datos Personales y su

reglamento de aplicación, las entidades financieras deben implementar mecanismos adecuados para ello, y que deben materializarse con formularios o formatos de solicitud de fácil entendimiento, brindando la información necesaria o especifica, que no induzca a engaños o confusiones, y que permitan satisfacer el requerimiento del titular. En este punto es trascendental brindar la información necesaria al consumidor sobre la definición del bloqueo o eliminación de datos personales, finalidades, mecanismos técnicos y operativos que permitan ejercer este requerimiento, así como medidas de seguridad que se implementan para el efectivo ejercicio del derecho.

La ausencia de desarrollo jurisprudencial y doctrinal en torno a la figura del bloqueo y anonimización en el marco de la Ley Orgánica y su Reglamento, genera un vacío jurídico que dificulta la aplicación y práctica de estos mecanismos. En este sentido, resulta crucial que la Superintendencia de Protección de Datos, en virtud de su facultad normativa (LOPDP, 2021, art. 4), emita las directrices claras y específicas que orienten a los responsables del tratamiento, en especial a las entidades del sistema financiero, sobre la correcta implementación de estas figuras. Dichas directrices deberán abordar, entre otros aspectos, la definición precisa, el alcance del bloqueo y de la anonimización, los criterios para la determinación de su aplicación, los procesos técnicos específicos a implementar y las medidas de seguridad a adoptar con el fin de garantizar efectivamente la protección de los datos personales.

Metodología

1. Objetivo General

Analizar la figura del bloqueo y anonimización de datos personales de consumidores bancarios, como parte del derecho de eliminación determinado por la Ley Orgánica de Protección de Datos y su Reglamento General de aplicación.

2. Objetivos Específicos

1. Determinar el régimen jurídico del derecho de eliminación de datos personales, en la legislación ecuatoriana.
2. Determinar el bloqueo o anonimización de datos personales dentro del derecho de eliminación establecido en la Ley Orgánica de Protección de Datos Personales.
3. Establecer los lineamientos sobre el bloqueo o anonimización de datos como alternativa a la aplicación del derecho de eliminación de Datos Personales de los consumidores bancarios.
4. Delimitar las regulaciones normativas que deberá expedir la Autoridad de Protección de Datos, para el correcto ejercicio del bloqueo o anonimización de datos personales de los consumidores bancarios.

3. Justificación y aplicación de la metodología

3.1. Nivel de estudio

Los autores de este documento aplicaron la metodología de investigación descriptiva, pues sus características permitieron delimitar conceptos, lineamientos; y, a partir del análisis descriptivo de los eventos relacionados con la eliminación de datos personales, logró estructurar de forma precisa los entregables, evidenciados en el proyecto de resolución emitida por la autoridad competente, así como el manual de tratamiento de datos personales encaminados a la anonimización o bloqueo.

3.2. Modalidad de investigación

La investigación para el desarrollo del proyecto de resolución y manual de tratamiento de datos personales descrito en el numeral anterior será documental, a efectos de obtener un producto que sirva como marco de referencia para las entidades bancarias, lo cual les permita entender y adoptar las mejores prácticas y procedimientos para la anonimización de datos personales, como alternativa jurídicamente valida ante el derecho de

eliminación, determinado por la norma en materia de protección de datos personales.

3.3. Método

El método a utilizarse en el presente proyecto es inductivo, pues permite obtener conclusiones y alternativas jurídicamente validas desde un análisis a las consideraciones generales de la problemática, y con ello obtener conclusiones específicas o particulares, que son de utilidad a las entidades bancarias, plasmadas en el proyecto de Resolución de la Superintendencia de Protección de Datos Personales, así como el manual para el tratamiento de datos personales en consumidores financieros, respecto la eliminación, bloqueo o anonimización de datos personales. El producto de esta investigación se basa en el articulado y normas ya especificadas sobre protección de la información personal de los consumidores financieros, y con ello presentar opciones que permitan hacer efectivos dichas disposiciones.

En este sentido, se ha utilizado encuestas y entrevistas como instrumento de recolección y tabulación de información, toda vez que permite reconocer descubrimientos, analizar de forma cualitativa y concisa la problemática, y reforzar la hipótesis planteada. Las entrevistas se han realizado a funcionarios de una entidad bancaria domiciliada en la ciudad de Quito; quienes, con sus conocimientos en gestión de data, derecho, seguridad de la información y tecnología, aportan a la elaboración de esta investigación. En relación a las entrevistas, se efectúan en el periodo del 15 de abril de los corrientes hasta la fecha actual, con el fin de obtener la retroalimentación necesaria; sin embargo, parte de los entrevistados han solicitado se mantenga reserva y no divulgación tanto de sus datos personales e identidad, así como la vinculación de su postura sobre el aspecto planteado, debido al desempeño de sus funciones en dicha entidad, motivo por el cual solicitaron suscribir un convenio de confidencialidad y no divulgación, que incluya la no transcripción del texto.

La estructura de las encuestas se enfoca a preguntas de carácter cerrado, cuyas características permiten centrar y abordar la problemática presentada en esta investigación, y son dirigidas a profesionales del derecho, colaboradores de la entidad y consumidores financieros.

3.4. Protocolo de investigación

Para el correcto desarrollo de este proyecto de titulación, se utilizarán los lineamientos establecidos por la metodología AGILE dada su característica de trabajo simétrico y eficiente, permitiendo dividir a la investigación en fases lógicamente ordenadas, junto con colaboración y mejora continuas de los autores, lo cual permitirá obtener resultados estructurados, abordando cada aspecto del desarrollo del presente proyecto.

4.- Propuesta de solución del problema identificado

4.1. Propuesta de Resolución de implementación de la anonimización o bloqueo de datos personales, por parte de la Autoridad de Protección de Datos.

Con la Ley Orgánica de Protección de Datos Personales en el 2021, se estableció un régimen común para garantizar el derecho a la protección de datos personales, que incluye el acceso y la decisión sobre información y datos de este carácter y su protección correspondiente (Asamblea Constituyente, Constitución de la República del Ecuador, 2008, art. 66 numeral 19), desarrollando principios, derechos, obligaciones y un mecanismo de tutela; pues es esencial que toda persona conozca las circunstancias que rodearán el tratamiento, destino y eliminación de datos. Así también, dispone en su artículo 15 que los titulares de datos personales pueden ejercitar el derecho de eliminación, agregando otros supuestos de hecho con el fin de hacer ilegible o dejar irreconocibles, determinando que la supresión no es la acción inequívoca de este derecho, sino que puede efectivizarse con otras acciones, dependiendo de los términos del contrato o los llamados intereses legítimos del artículo 7 de la mencionada Ley (Asamblea Nacional del Ecuador, LOPDP, 2021).

Es así, que el Reglamento de la Ley Orgánica de Datos Personales (Presidencia de la República del Ecuador, 2023) dispone en su artículo 9 y 11 que también puede bloquearse o anonimizarse datos personales, así como agrega supuestos de hecho donde no proceden la eliminación, en este sentido mediante una interpretación sistemática entre la Ley y el Reglamento, las acciones de hacer ilegible o dejar irreconocibles están asociados con el bloqueo y la anonimización, las cuales no han sido analizadas por los órganos administrativos o judiciales competentes.

La Corte Constitucional en la Sentencia No. 1868-13-EP/20 (08 de julio de 2020) definió la eliminación como la acción de suprimir la información de carácter personal que está en registros, archivos, documentos o cualquier base de datos ya sea privada o pública, lo que implica desaparecer la información ya sea física o digital e impedir su recuperación. Sin embargo, existen excepciones para el ejercicio del derecho de eliminación, una de ellas es que exista una obligación legal de conservarla (Presidencia de la República del Ecuador, RLOPDP, 2023, art. 9). Para objeto del presente estudio, se tomará en cuenta lo establecido en el artículo 225 del Código Orgánico Monetario y Financiero (2014), cuyo texto establece que toda entidad que conforme el sistema financiero nacional, mantendrá sus archivos contables físicos, incluyendo los respaldos respectivos, por el plazo de diez años contados a partir de la conclusión de la operación correspondiente y por quince años en el formato digital autorizado por las superintendencias (Asamblea Nacional del Ecuador, 2014). En este caso, existe una disposición legal que permite a las instituciones financieras mantener archivos por más tiempo, incluso pese a la petición de eliminación realizada por el titular. Sin embargo, es trascendental traer a colación ciertas particularidades que distinguen al sector financiero del resto sobre quienes recae la aplicación de estas normas; dada la permanente, rigurosa y excesiva regulación normativa incorporada.

Para efectos de este análisis, se entenderá al bloqueo de datos de consumidores bancarios como el de los personales en un archivo físico o digital, pero restringiendo su acceso, permitiendo que solo personas autorizadas accedan a los datos, es decir, el bloqueo se utilizará como una medida temporal de carácter cautelar, restringiendo su tratamiento, más no su almacenamiento, para suprimir o anonimizar el dato, siempre que se cumplan los supuestos taxativos del artículo 15 de la Ley, cuando es imposible borrar las bases de datos.

En cambio, la anonimización de datos de consumidores bancarios se entenderá como proceso sustitutivo del derecho de eliminación, en el cual se romperá el vínculo entre el dato personal y la identificación del titular, sin eliminar la base de datos original, puesto que es necesario para el proceso de reidentificación justificando en un interés legítimo y lícito del Responsable del tratamiento, si permite al igual que el bloqueo, la imposibilidad de que una persona no autorizada o el público (con bases de datos públicas) puedan identificar al titular atentando contra su derecho a la intimidad u honor, momentáneamente. En este punto, es menester hablar sobre la seudonimización, esta medida de seguridad tiene la necesidad de usar dos encargados de datos personales dentro del mismo organismo o equipos separados para manejar las bases de datos, pero bajo la dirección de un mismo responsable y por ende con fines iguales.

Para mejor entendimiento de estas definiciones, se realiza un cuadro comparativo, entre estas dos figuras:

Tabla 1:

Tabla comparativa entre el bloqueo y anonimización de datos personales.

Características	**Bloqueo**	**Anonimización**
Finalidad	Impedir el tratamiento temporal de datos.	Disociar la información del titular,

		imposibilitando su identificación.
Reversibilidad	Reversible, se puede volver a acceder a los datos	Irreversible, la información no se puede asociar al titular
Acceso a los datos	Restringido a personas autorizadas.	No se puede identificar al titular, incluso con información adicional
Ejemplo	Retener datos de un cliente que solicite eliminación, pero con una deuda pendiente.	Transformar datos de transacciones para análisis estadístico agregado.

Nota: Tabla comparativa entre el bloqueo y anonimización de datos personales, para la aplicación por parte de las entidades financieras. **Fuente:** Elaboración propia

Para la correcta aplicación del bloqueo y anonimización, se requiere de personal capacitado por la entidad bancaria, quienes deberán ponderar y evaluar el interés legítimo del responsable del tratamiento que deberá ser necesario y proporcionado, según el Reglamento de la Ley Orgánica de Protección de Datos Personales (Presidencia de la República del Ecuador, 2023, art. 7), con el fin de evitar emitir actos discrecionales, quienes deberán tomar en cuenta que no todas las normas o principios jurídicos tienen el mismo valor o importancia. Algunos principios, como los derechos fundamentales, pueden tener un peso mayor que otros principios.

4.1.1. Proyecto de Resolución que regule la aplicación de bloqueo o anonimización de datos personales en consumidores bancarios. Corresponde a la máxima autoridad de la Superintendencia de Protección de Datos Personales emitir las resoluciones para proteger los derechos y libertades fundamentales de tratamiento de datos personales de las personas naturales. (Asamblea Nacional del Ecuador, LOPDP, 2021, art. 4) Esta atribución normativa de carácter administrativo le permite regular los asuntos del órgano a su cargo (Asamblea Nacional del Ecuador, COA, 2017, art. 130).

Como sucede en materia financiera con los órganos de regulación como la Junta de Política y Regulación Financiera, Junta de Política y Regulación Monetaria y la Superintendencia de Bancos como órgano de control, tienen la atribución de establecer normas jurídicas técnicas y operativas que complementan las disposiciones del Código Orgánico Monetario y Financiero, lo que incluye la supervisión permanente del cumplimiento de estas; es esencial que la autoridad de protección de datos se alinee a la normativa secundaria relacionada con sus funciones, lo que le permitirá mantener una adecuada gestión de regulación y control sobre sus supervisados.

Si bien, no existe normativa específica para la creación de estos actos normativos de carácter administrativo, para una redacción clara y correcta de este proyecto resolutivo, se utilizará el Manual de Técnica Legislativa, con el fin de que la Autoridad de Protección de Datos pueda construir esta herramienta regulatoria de utilidad práctica, teórica y conceptual, para vigilar, auditar, intervenir, proteger y controlar las actividades atribuidas en la Ley.

Como primer punto, tendremos los considerandos en los cuales se especificará las normas constitucionales, legales, reglamentarias y demás resoluciones en sucesión jerárquica que fundamentarán la pertinencia del proyecto de regulación. Una vez concluidos los considerandos, daremos paso a las disposiciones preliminares o directivas, en el cual desarrollaremos “mínimamente el objeto, finalidad, ámbito de aplicación, principios y

definiciones” conforme consta en el Reglamento de Técnica Legislativa (Consejo de Administración Legislativa, 2021, Art. 22, literal a).

Una vez definidos los objetivos y riesgos, así como la viabilidad del proceso, una tarea esencial será la de definir un esquema basado en los tres niveles de identificación de personas: microdatos, identificadores indirectos y datos sensibles (principio de proactividad), donde se asigne un valor cuantitativo a cada una de las variables. Esta escala debe ser conocida por todo el personal implicado (principio de información) y es crítico para la Evaluación de Impacto en la Protección de los Datos Personales (EIPD).

El procedimiento que la institución bancaria deberá seguir para ejercer el derecho de eliminación y por ende al de bloqueo o anonimización de los consumidores financieros, conforme a la Ley y el Reglamento, es el siguiente:

1. El cliente financiero o quien tenga la facultad legal de representar al interesado o consumidor afectado, presentará la solicitud de eliminación, esta solicitud deberá ser de manera escrita.
2. Deberá presentar su solicitud ante la institución financiera de la cual es cliente o consumidor, sea a través de agencias físicas o los demás canales que para tal efecto determine el responsable.
3. Una vez receptada la solicitud por el encargado, este procederá a bloquear el dato sobre el cual se presentó la reclamación.
4. En caso de que el responsable de la información requiera que la solicitud sea aclarada o ampliada, podrá requerir al titular, por una sola vez y dentro del término de cinco (5) días de recibida la solicitud, que la aclare o complete.
5. El recurrente tendrá el término de diez (10) días contados a partir del día siguiente a la notificación, para aclarar o completar la solicitud.
6. La entidad financiera, dentro del término de diez (10) días de presentada o aclarada la solicitud, deberá resolverla admitiéndola o rechazándola motivadamente. Esta resolución deberá ser notificada en los lugares señalados para el efecto por el recurrente.

7. En el caso que la resolución sea favorable, el encargado procederá a la anonimización o seudoanonimización del dato del cliente bancario.
8. Al no estar conforme con la resolución o de existir negativa por parte del responsable o encargado del tratamiento de datos personales, el titular podrá recurrir ante la Autoridad de Protección de Datos Personales, quien deberá notificar de esta impugnación al responsable, a fin de mantener bloqueado el dato hasta la resolución del procedimiento administrativo.

Tras desarrollar el procedimiento y el régimen sancionatorio, se redactarán las disposiciones finales, artículos al final del texto normativo y regulan aspectos relacionados con su aplicación, vigencia y derogación. Cabe señalar que, dentro de la normativa, no se incluirá disposiciones derogatorias, puesto que, al ser una entidad administrativa recién creada, no existen normas previas que derogar, razón por la cual es indispensable que cuente con un plan de implementación sólido, que incluya capacitación del personal, asignación de recursos adecuados, estrategias de gestión del cambio y una estrecha coordinación interinstitucional.

4.1.2. Proyecto de manual para el tratamiento de datos personales en consumidores financieros, respecto eliminación, bloqueo o anonimización de datos personales.

Para el desarrollo de este apartado, es de especial relevancia referirnos brevemente a las disposiciones normativas sobre bloqueo y anonimización en nuestra legislación frente a lo que señala el Reglamento de Datos Personales de la Unión Europea (GDPR), y con este análisis comprender los sustentos necesarios para diseñar un proceso adecuado que permita garantizar la aplicación efectiva de estos mecanismos conforme especificaciones técnicas y normativas.

En este sentido, el Art. 37 de la LOPDP determina las obligaciones del responsable del tratamiento en cuanto la seguridad de datos personales,

puntualizando la aplicación de mecanismos de seguridad idóneas, como la anonimización, seudonomización o cifrado de datos personales. En línea con esto, el artículo 9 del Reglamento de aplicación a la antedicha ley señala que:

> “Cumplida la o las finalidades del tratamiento y cuando no exista disposición legal o reglamentaria o no incurra la necesidad de mantener los datos en virtud del interés legítimo del responsable, o por cumplimiento de una obligación legal que establezca lo contrario, el responsable deberá proceder a la eliminación, bloqueo o anonimización de los datos en su posesión”. (Presidencia de la República del Ecuador, 2023, art. 9)

Con ello, podemos comprender la obligación de las entidades bancarias de establecer mecanismos de seguridad que impidan la identificación de los titulares cuando se cumplan los supuestos que determina la norma, pero dicha disposición se vuelve un tanto inaplicable, cuando el mismo reglamento no es del todo coherente en sus conceptos; toda vez que, el derecho de eliminación debe ser aplicado en los términos estrictos del artículo 11 del reglamento; es decir, proceder a la eliminación segura de los datos personales, entendiendo a este concepto como la forma de tratamiento de datos que elimine las bases de datos sin opción a recuperación o de forma sustitutiva se aplique el bloqueo o anonimización asegurando la privacidad del titular o la creación de datos anonimizados que impidan la identificación del sujeto de derechos.

Es aquí cuando se pueden generar varias interpretaciones no concretas sobre la aplicación al derecho de eliminación; pues el cuándo permite implementar mecanismos alternativos como la anonimización o bloqueo de datos personales; sin embargo, nuestro ordenamiento jurídico no contempla técnicas, procesos o mecanismos específicos para su aplicación, lo que motiva la consulta a documentos académicos que puedan sugerir lineamientos adecuados.

En este sentido, si bien el Parlamento Europeo y el Consejo de la Unión Europea (Reglamento (UE) 2016/679, 2016) mediante el Reglamento General

de Protección de Datos de la Unión Europea no cuenta con artículos específicos a la anonimización de datos personales, pero si aborda esta institución en varias de sus disposiciones legales, partiendo de la definición de dato personal que contiene el artículo 4, así como el principio de protección por diseño y defecto que especifica el articulo 25 ibidem, al establecer como obligación de los responsables el contar con medidas operativas y técnicas como la seudonimización (concepto derivado de anonimización) o cifrado de datos.

Para concretar el análisis de la descripción arriba señalada, es preciso referirnos al contenido del considerando 26 del GDPR, pues trata de desligar a la información anónima de los principios de protección, pues ya no se podría considerar como dato personal a la información que no identifique o haga identificables a los titulares; es decir, ¨información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo¨ (Parlamento Europeo y el Consejo de la Unión Europea, Reglamento (UE) 2016/679, 2016).

A pesar de la ausencia de normativa específica sobre anonimización en el GDPR, encontramos textos académicos de entidades colegiadas como la Asociación Española de Protección de Datos, cuyos aportes nutren a la normativa relacionada con la privacidad de datos de los ciudadanos de los países miembros de la Unión Europea; en este sentido, dicha entidad ha elaborado documentos sustancialmente importantes en lo que a anonimización se refiere.

En este sentido, la *Guía de Introducción a la anonimización de datos. Técnicas y casos prácticos* de la Asociación Española de Datos Personales, plantea ciertos principios como consideraciones previas a la aplicación de este procedimiento. Aunque su texto es extenso e ilustrativo, vale la pena enunciar al Principio proactivo, Principio de privacidad por defecto, Principio objetivo, Principio funcional, Principio integral, Principio de información y Principio

Atómico, cuyas definiciones se condensan en la protección de la información de los titulares durante todo el ciclo de vida del dato, con la identificación plena de las finalidades de dicho proceso, preservando la confidencialidad, una adecuada evaluación de riesgos ante una reidentificación del dato anonimizado, sumado a la especificación de roles y criticidad de estos, sin olvidar la capacitación constante de los involucrados en dicho proceso (Asociación Española de Datos Personales, 2022).

La investigación se ha realizado también en derecho comparado, y atendiendo a las realidades de cada legislación como la mexicana; sin embargo, no se evidencia sustento similar o distinto sobre la aplicación de los principios para la adecuada gestión de anonimización de datos personales, aunque si aplican los principios generales de protección de la información, encaminados a cada uno de los mecanismos técnicos y operativos, lo que garantiza el ejercicio de derechos y demás aspectos señalados por su normativa.

Ahora bien, lo mismo sucede cuando encontramos sustentos jurídicos respecto lineamientos para aplicar técnicas de anonimización, sin embargo, la misma Asociación Española de Datos Personales (2022) a través de la Guía básica de anonimización sugiere varias técnicas, que se describen a continuación:

a) Supresión de registros
b) Supresión de atributos
c) Enmascaramiento de caracteres:
d) Generalización
e) Perturbación de datos

Es por lo que, las técnicas aquí descritas, en su afán de proteger la privacidad de los titulares, requieren de la instrumentación de un proceso de anonimización, que garantice la efectividad y el cumplimiento de las normativas de protección de datos. Sin embargo, se pueden utilizar otros mecanismos derivados, como la tokenización, agregación de datos y el cifrado

o encriptación de datos, siempre que dicho mecanismo tenga por finalidad no solo disociar al dato, sino impedir su re identificación, para de esa forma garantizar el ejercicio del derecho del consumidor financiero.

Estos antecedentes nos permiten comprender la pertinencia de la aplicación de la anonimización de datos personales, sin olvidar el bloqueo previo como una medida de carácter preventivo, lo cual motiva la necesidad de elaboración de un instrumento metódico y documentado para la aplicación efectiva del derecho a la eliminación, siempre que para este fin exista la motivación jurídica debida, dada por la LOPDP, su reglamento de aplicación, así como la correspondiente resolución que emita la autoridad respectiva.

Conclusiones y Recomendaciones

1. Conclusiones

Es necesaria la emisión de la Resolución que regule la aplicación del derecho de eliminación y por ende la figura del bloqueo y anonimización de datos personales en consumidores bancarios, por parte de la máxima autoridad de la Superintendencia de Protección de Datos Personales, por cuanto garantiza el derecho fundamental a la protección de datos personales de los consumidores bancarios, consagrado en la Constitución de la República del Ecuador, en la Ley Orgánica de Protección de Datos Personales y su Reglamento General. La resolución empoderaría a los consumidores financieros a ejercer control sobre su información personal y limita la capacidad de las entidades bancarias para utilizarla sin su consentimiento o para fines no autorizados.

Así también, es necesario que las entidades que conformen el Sistema Financiero Nacional establezcan mecanismos claros y precisos para el correcto ejercicio de la anonimización o el bloqueo de datos personales en sus políticas o manuales internos, para ello deben poseer directrices claras por parte de la Autoridad administrativa que permitan fortalecer la seguridad jurídica en el ámbito de la protección de datos personales financieros.

La figura del bloqueo se deberá utilizar como una medida temporal cautelar, restringiendo el tratamiento del dato en la institución financiera, más no su almacenamiento, si culmina el plazo de prescripción legal o contractual o cuando exista una petición del interesado que deba analizarse por la entidad bancaria.

Para la anonimización y seudoanonimización, la ley ecuatoriana lo ha colocado como el tratamiento de separar a la información y los datos personales generando dos bases de datos distintas que solo pueden volver individualizar al titular cuando se combinan, lo que implica la posibilidad de re identificar al titular. Si bien la anonimización se presenta como un mecanismo robusto para proteger la privacidad, el auge del Big Data e inteligencia artificial plantean nuevos desafíos, pues la capacidad de esta tecnología para analizar grandes conjuntos de datos y encontrar patrones ocultos, pueden socavar la efectividad de la anonimización.

2. Recomendaciones

Se recomienda a la máxima autoridad de la Superintendencia de Protección de Datos Personales conforme a sus atribuciones normativas de carácter administrativo establecidas en la Ley Orgánica de Protección de Datos Personales, su Reglamento General y el Código Orgánico Administrativo, emita la resolución que regule la aplicación de bloqueo o anonimización de datos personales en consumidores bancarios. La propuesta ayudará a garantizar que las entidades financieras traten de manera responsable y segura los datos personales de sus clientes.

El objetivo de esta resolución es que la Autoridad de Protección de datos personales brinde las directrices que protejan los derechos de los consumidores financieros en relación con sus datos personales. La propuesta establece una serie de medidas que las entidades financieras deberán considerar para anonimizar o bloquear los datos personales a petición de parte o cuando esta información ha cumplido con el propósito para el que fue recolectado.

Con la expedición de esta Resolución, las instituciones bancarias obtendrán los elementos necesarios para implementar o perfeccionar su política de protección de datos personales, con un apartado sobre el bloqueo y anonimización de datos personales. Los bancos, como entidades que manejan información financiera sensible de sus clientes, tienen la obligación legal y ética de implementarla, estableciendo de manera particular los mecanismos para que los consumidores financieros puedan ejercer estos derechos. La implementación de un manual adecuado de tratamiento de datos personales demuestra el compromiso de la entidad financiera con la protección de la privacidad de sus clientes y contribuye a generar confianza en ellos.

Referencias

Agencia Española de Protección de Datos. (2022). *Guía básica de anonimización. Elaborada por Autoridad Nacional de Protección de Datos de Singapur*. https://www.aepd.es/documento/guia-basica-anonimizacion.pdf

Alcalá, J. A. del R. (2020). El Derecho a la Tutela Judicial Efectiva: Teoría General. En F. L. Yagüe, I. F. B. Ortúzar, & J. M. Díaz (Eds.), *Garantías de los derechos en el nuevo panorama constitucional cubano.* (pp. 21–38). Dykinson, S.L. https://doi.org/10.2307/j.ctv103x9wq.5

Asamblea Constituyente. (2008). *Constitución de la Republica del Ecuador* (CRE). Registro Oficial No. 449, 20 de octubre de 2008.

Asamblea Nacional del Ecuador (2014). *Manual de Técnica Legislativa* (2da ed.). https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-20/publicaciones/manual-tecnica-legislativa.pdf

Asamblea Nacional del Ecuador (2022). *Ley Orgánica de Protección de Datos Personales (LOPDP)*. Registro Oficial Quinto Suplemento No. 459, 26 mayo 2021. https://www-fielweb-

com.bibliotecavirtual.udla.edu.ec/Index.aspx?rn=38135&nid=1162059#norma/1162059

Asamblea Nacional del Ecuador. (2009). *Ley Orgánica de Garantía Jurisdiccionales y Control Constitucional*. Registro Oficial Suplemento 52, 22 de octubre de 2009.

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Monetario y Financiero, Libro I*. Registro Oficial Suplemento 332, 12 de septiembre de 2014.

Asamblea Nacional del Ecuador. (2016). *Ley Orgánica de Gestión de la Identidad y Datos Civiles (Reformada)*. Registro Oficial Suplemento No. 684, 04 febrero 2016. https://strapi.lexis.com.ec/uploads/Reforma_939ec3ac5e.pdf

Asamblea Nacional del Ecuador. (2017). *Código Orgánico Administrativo*. Registro Oficial Suplemento 31, 07 de julio de 2017.

Ayuso, J. F. R. (2019). Principios de protección de datos. En *Figuras y responsabilidades en el tratamiento de datos personales* (1ra ed., pp. 27–74). J.M Bosch. https://doi.org/10.2307/j.ctvwcjghh.5

California Consumer Privacy Act. (2018). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

Cámara de Diputados del Honorable Consejo de la Unión. (5 de julio de 2010). *Ley Federal de Protección de Datos Personales en Posesión de Particulares.* Diario Oficial de la Nación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Congreso Nacional. (1994). *Ley General de Instituciones del Sistema Financiero*. Registro Oficial Suplemento No. 52, 22 de octubre de 2009.

Consejo de Administración Legislativa. (18 de febrero de 2021). Resolución CAL-2019-2021-419. *Reglamento de Técnica Legislativa*.

https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-20/UTL/2022/2.-REGLAMENTO-TECNICA-LEGISLATIVA.pdf

Córdova, J. (2023). *Filtración Masiva de Datos en Ecuador y el Rol de la Ley de Protección de Datos*. https://www.linkedin.com/pulse/filtraci%C3%B3n-masiva-de-datos-en-ecuador-y-el-rol-la-ley-cordova-l%C3%B3pez/

Corte Constitucional del Ecuador. (08 de julio de 2020). Sentencia No. 1868-13-EP/20. http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOicyNzE4ZjljZC1hZjU4LTQxMTItYjBkYi01MjVlYmUwNDU2ZjgucGRmJ30=#:~:text=una%20sentencia%20expedida%20en%20un,naturaleza%20de%20esta%20garant%C3%ADa%20jurisdiccional

El Comercio. (16 de septiembre de 2019). BBC revela filtración de datos sensibles de millones de ecuatorianos. *El* Comercio. https://www.elcomercio.com/tendencias/tecnologia/datos-ecuatorianos-filtracion-reporte-seguridad.html

Instituto Interamericano de Cooperación para la Agricultura. (2023). *Manual de Procedimientos sobre la protección de datos personales*. https://repositorio.iica.int/handle/11324/18806

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México (INAI). *Guía de mejores prácticas en materia de protección de datos personales con un enfoque practico Sector Público*. https://home.inai.org.mx/wp-content/uploads/Gu%C3%ADa_Mejores-pr%C3%A1cticas_SP.pdf

Jefatura del Estado de España. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Boletín Oficial del Estado Núm. 294, Sec. 1, Pág.

119788,6 de diciembre de 2018. https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

Lasso Roldan, E. (2024). Incidencia de la anonimización de base de datos en el cumplimiento de la Ley de Protección de Datos Personales en el Ecuador. *Ibero-American Journal of Engineering & Technology Studies, 4* (1) 71-76. https://tech.iberojournals.com/index.php/IBEROTECS/article/view/642/476

Milanes, V. (2017). Desafíos en el debate de la protección de datos para Latinoamérica. *Revista Transparencia & Sociedad*, (5), 13 – 31. https://www.consejotransparencia.cl/wp-content/uploads/2018/04/v_milanes__1_.pdf#:~:text=Para%20avanzar%20en%20el%20an%C3%A1lisis%20sobre%20la%20protecci%C3%B3n,vez%20m%C3%A1s%20creciente%20trans-ferencia%20internacional%20de%20datos%20personales

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). Acuerdo Ministerial 35. *Guía de datos abiertos de aplicación en Administración Pública Central*. Registro Oficial Suplemento No. 371, 15 de enero de 2021. Guia-Datos-Abiertos-con-portada.pdf (www.gob.ec)

Ordoñez Pineda, L., Correa Quezada, L., y Correa Conde, A. (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

Parlamento Europeo y Consejo de la Unión Europea. (24 de octubre de 1995). *Directiva 95/46.* https://www.oas.org/es/sla/ddi/docs/Directiva-95-46-CE.pdf

Parlamento Europeo y el Consejo de la Unión Europea. (27 de abril de 2016). Reglamento (UE) 2016/679. *Reglamento General de Protección de Datos (RGPD)*. Diario Oficial de la Unión Europea L 119/1. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Presidencia de la República del Ecuador (2023). Decreto Ejecutivo No. 904. *Reglamento de la Ley Orgánica de Protección de Datos Personales*. Registro Oficial Tercer Suplemento No. 435 de 13 de noviembre de 2023. Ediciones Legales EDLE S.A. https://www-fielweb-com.bibliotecavirtual.udla.edu.ec/Index.aspx?rn=38135&nid=1184318#norma/1184318

Presidencia de la República del Ecuador. (16 de marzo de 2020). *Decreto Ejecutivo No. 1017*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/03/Decreto_presidencial_No_1017_17-Marzo-2020.pdf

Presidencia de los Estados Unidos Mexicanos. (21 de diciembre de 2011). *Reglamento a la Ley Federal de Protección de Datos Personales en Posesión de Particulares.* Diario Oficial de la Nación. https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Secretaria de Estado de Digitalización e Inteligencia Artificial de España (2022). *Introducción a la anonimización de datos. Técnicas y casos prácticos.* https://datos.gob.es/sites/default/files/doc/file/informe-anonimizacion-es.pdf

Superintendencia de Bancos. (16 de febrero de 2024). Resolución No. SB-2024-0316. *Norma de Control para la Administración del Riesgo de Lavado de Activos y Financiamiento del Terrorismo, y Financiamiento a la Proliferación de Armas de Destrucción Masiva (ARLADFT).* https://asobanca.org.ec/wp-content/uploads/2024/03/Resolucion-SB-2024-0316-Reforma-la-Norma-de-Control-ARLAFDT.pdf

Superintendencia de Bancos. (2017). Resolución 810. *Codificación de las Normas de la Superintendencia de Bancos, Libro I. – Normas de Control para las entidades de los sectores financieros público y privado, Título IX. – de la Gestión y Administración de Riesgos, Capítulo V, Norma de control para la gestión de riesgo operativo*. Registro Oficial Edición Especial 123, 31 de octubre de 2017. https://www.superbancos.gob.ec/bancos/codificacion-de-normas-de-la-sb-libro-uno-sistema-financiero/

Superintendencia de Bancos. (2024). Resolución SB-2024-0316 de 16 de febrero de 2024. *Codificación de las Normas de la Superintendencia de Bancos, Libro I. – Normas de Control para las entidades de los sectores financieros público y privado, Título IX. – de la Gestión y Administración de Riesgos, Capítulo VI, Norma de control para la administración del riesgo de lavado de activos y financiamiento del terrorismo, y financiamiento a la proliferación de armas de destrucción masiva (ARLADFT)*. https://www.superbancos.gob.ec/bancos/codificacion-de-normas-de-la-sb-libro-uno-sistema-financiero/

Anexos

Anexo I

Resolución No. SPDP-2024-XXX
Dr. Fabrizio Roberto Peralta Díaz
SUPERINTENDENTE
SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES

Considerando:

Que, el numeral 19 del artículo 66 de la Constitución de la República reconoce y garantiza el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección;

Que, el numeral 6 del artículo 76 de la Carta Magna determina que "*En todo proceso que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas: 6. La ley establecerá la debida proporcionalidad entre las infracciones y las sanciones penales, administrativas o de otra naturaleza*";

Que, el artículo 92 de la Norma Suprema prescribe que, toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o

de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados";

Que, el artículo 226 de la Constitución de la República del Ecuador, dispone: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrá el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución"*;

Que, el articulo 225 del Código Orgánico Monetario y Financiero estable que las entidades del sistema financiero nacional mantendrán sus archivos contables físicos, incluyendo los respaldos respectivos, por el plazo de diez años contados a partir de la conclusión de la operación correspondiente y por quince años en el formato digital autorizado por las superintendencias.

Que, el artículo 47 del Código Orgánico Administrativo, prescribe: La máxima autoridad administrativa de la correspondiente entidad pública ejerce su representación para intervenir en todos los actos, contratos y relaciones jurídicas sujetas a su competencia. Esta autoridad no requiere delegación o autorización alguna de un órgano o entidad superior, salvo en los casos expresamente previstos en la ley;

Que, en el Quinto Suplemento del Registro Oficial No. 459 de 26 de mayo de 2021, se expidió la Ley Orgánica de Protección de Datos Personales, en cuyo artículo 2 se dispone que la Ley regula el tratamiento de datos personales contenidos en cualquier tipo de soporte;

Que, el artículo 4 de la Ley ibidem, define a la Autoridad de Protección de Datos Personales, como: *"Autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales".*

Que, el literal c) del numeral del articulo 29 de la misma Ley, sobre los derechos de los Titulares de Datos Crediticios, garantiza el derecho a que las fuentes de información actualicen, rectifiquen o eliminen, según el caso, la información que fuese ilícita, falsa, inexacta, errónea, incompleta o caduca.

Que, mediante Decreto Ejecutivo No. 904 de 06 de noviembre de 2023, el presidente de la República del Ecuador expide el REGLAMENTO GENERAL DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES, publicado en el Registro Oficial Tercer Suplemento No. 435, de fecha 13 noviembre de 2023).

Que, conforme a las atribuciones normativas de carácter administrativo establecidas en la Ley Orgánica de Protección de Datos Personales y Código Orgánico Administrativo, es menester emitir la resolución que regule la aplicación de bloqueo o anonimización de datos personales en consumidores bancarios, por lo cual,

Resuelve:

EXPEDIR LA NORMA PARA APLICAR EL BLOQUEO Y ANONIMIZACIÓN DE DATOS PERSONALES EN CONSUMIDORES BANCARIOS

Capítulo I

APLICACIÓN, PRINCIPIOS Y DEFINICIONES

Articulo 1.- Objeto. - La presente Resolución regula la correcta aplicación del bloqueo y anonimización de datos personales de los consumidores financieros en las instituciones que conforman el Sistema Financiero Nacional.

Artículo 2.- Finalidad. - Garantizar a los consumidores financieros, el derecho de obtener del responsable del tratamiento, el correcto ejercicio del bloqueo o anonimización de los datos personales, cuyo tratamiento se ajuste a las disposiciones de la presente resolución.

Artículo 3.- Ámbito de aplicación. - La presente Resolución será de aplicación obligatoria por las entidades financieras que conforma el Sistema Financiero Nacional y que trata datos personales de consumidores financieros.

Artículo 4.- Definiciones. - Además de las definiciones establecidas en la Ley de Protección de Datos Personales y su Reglamento General, para efectos de la presente Resolución, se establecen las siguientes definiciones:

Bloqueo: identificación y conservación de datos personales una vez cumplida la finalidad para la que se recabaron, para determinar responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de estas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.

Cliente: Persona natural o jurídica que mantiene una relación contractual con una o varias de las instituciones que conforman el Sistema Financiero Nacional, respecto de los productos y servicios que ofrece.

Consumidor financiero: Se refiere a los clientes y usuarios que mantienen una relación contractual con una o varias instituciones del Sistema Financiero Nacional o consumen los servicios de orden público que estas entidades brindan.

Datos personales de consumidores financieros: Información sobre una persona natural o jurídica cuya identidad pueda determinarse, directa o indirectamente, mediante un identificador, nombre, razón social, número de identificación, datos de localización, o elementos propios de su identidad, como datos biométricos, en el caso de personas naturales, o generados por

una relación contractual y/o utilización de los productos y servicios de la entidad financiera. Se exceptúa de esta definición a los datos personales de categoría sensible, así como a todo tipo de dato personal generado en material audiovisual, por las cámaras de seguridad o circuito cerrado de televisión, respecto de los consumidores financieros al momento de ingresar, utilizar o permanecer en sus instalaciones, de acuerdo con sus Políticas de seguridad e infraestructura física.

Sistema Financiero Nacional: Se compone de los sectores público, privado y del popular y solidario, que intermedian recursos del público.

Usuarios financieros: Personas naturales o jurídicas que no mantienen una relación contractual con la entidad financiera, pero utilizan los productos y servicios financieros que la Entidad oferta.

Capítulo II

GENERALIDADES

Artículo 5.- Medios para el ejercicio de los derechos. - Las instituciones que conformen el Sistema Financiero Nacional habilitarán, preferentemente, herramientas o canales informáticos simplificados de fácil acceso para el titular, con la finalidad de receptar y atender oportunamente las solicitudes o peticiones formuladas que permitan y garanticen una interacción segura, fiable y rápida entre el responsable y el titular, sin perjuicio de que también puedan ser presentadas por medios físicos.

Artículo 6.- Contenido de la solicitud. - En la solicitud para el ejercicio de los derechos consagrados en la Ley, se hará constar:

1. Los nombres y apellidos completos del titular, número de cédula de identidad o pasaporte y dirección domiciliaria o electrónica para notificaciones. Cuando se actúa en calidad de representante legal, se hará constar también los datos de la o del representado;
2. De ser posible, la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados y cualquier otro elemento o documento que facilite la

localización de los datos personales;
3. Relación de lo que solicita expuesto de manera clara y precisa;
4. Derecho o derechos que desea ejercer; y,
5. A la solicitud se acompañará los documentos que acrediten la identidad o, en su caso, la representación legal o convencional del titular.

Artículo 7.- Requerimiento de información adicional. - En caso de que la información constante en la solicitud requiera ser aclarada o ampliada, el responsable podrá requerir al titular, por una sola vez y dentro del término de cinco (5) días de recibida la solicitud, que la aclare o complete.
El titular emplazado contará con el término de diez (10) días contados a partir del día siguiente en el que haya sido notificado, para aclarar o completar la solicitud.
Si el titular aclara o completa la solicitud dentro del término concedido, el responsable le dará la debida atención, caso contrario, la archivará notificando este particular al titular con las razones de su decisión. El archivo del requerimiento inicial no impedirá la presentación de una nueva solicitud.

Artículo 8.- Registro de solicitudes. - El responsable deberá registrar todas las solicitudes de ejercicio de derechos, incluyendo el detalle de la atención dada a las mismas.

Artículo 9.- Reclamo ante la Autoridad de Protección de Datos Personales.- El titular de datos personales que encuentre motivos para creer que se han vulnerado sus derechos con la respuesta que el responsable ha dado a su solicitud, o que no haya recibido respuesta en el plazo establecido, podrá acudir a la Autoridad de Protección de Datos a presentar su reclamo, el cual se sustanciará conforme al procedimiento previsto en el Código Orgánico Administrativo y en la normativa complementaria que, para el efecto, emita la Autoridad de Protección de Datos.

El procedimiento de reclamo contemplará la notificación al responsable para que ejerza su derecho a la defensa.

Capítulo III

DEL BLOQUEO DE DATOS PERSONALES DE CONSUMIDORES FINANCIEROS

Artículo 10.- Derecho a la suspensión del tratamiento. - El titular de datos financieros tendrá derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a. Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de estos;
b. El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
c. El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; y.
d. Cuando el interesado se haya opuesto al tratamiento en virtud del artículo 31 de la presente ley; mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica su exactitud, deberá el responsable bloquear el dato inconforme del titular.

Artículo 11. - Responsable. - El responsable del tratamiento estará obligado a bloquear los datos cuando se solicite su rectificación o eliminación y mientras dure su resolución.

Artículo 12. - Medidas técnicas y organizativas. - Las instituciones financieras adoptarán medidas técnicas y organizativas, para impedir el tratamiento de los datos personales bloqueados, incluyendo su visualización, excepto para la puesta a disposición a solicitud de Autoridades Judiciales, Constitucionales, Servicio de Rentas Internas o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la

exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de estas.

Artículo 13.- Solicitud. - El titular tendrá en todo momento el derecho a presentar la solicitud de rectificación o eliminación de sus datos personales. La solicitud dará lugar a un periodo de bloqueo tras el cual se procederá al análisis por parte del responsable de la institución. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento.

Artículo 14.- Duración. - El periodo de bloqueo no podrá exceder al de resolución del requerimiento de eliminación o mientras dure la impugnación. Una vez eliminado, anonimizado o seudoanonimizado el dato, se dará aviso a su titular.

Artículo 15.- Configuración del sistema de información. - Cuando la configuración del sistema de información no permita el bloqueo o se requiera una adaptación con esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de esta, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

Capítulo IV

DE LA ANONIMIZACIÓN DE DATOS PERSONALES DE CONSUMIDORES FINANCIEROS

Artículo 16.- Aplicación de la anonimización.- Cuando exista disposición legal, reglamentaria o contractual, que impida la eliminación del dato del consumidor financiero, una vez cumplida la finalidad del dato el responsable deberá proceder a la anonimización de los datos en su posesión.

Artículo 17.- Principios. - La anonimización de datos personales de consumidores financieros deberá regirse bajo los principios de legalidad, finalidad, seguridad.

Artículo 18.- Medidas de anonimización.- La anonimización de datos de consumidores financieros debe regirse por el concepto de privacidad desde el diseño y por defecto, de no hacerlo será considerado como falta grave.

Artículo 19.- Técnicas de anonimización.- La entidad financiera deberá implementar técnicas de anonimización en sus políticas, sin menoscabar el derecho de las personas al respeto a la protección de sus datos personales.

Artículo 20.- Requisitos para la anonimización.- Las entidades financieras deberán cumplir con los siguientes requisitos para la anonimización de datos personales de consumidores financieros:

a) Eliminar cualquier información que permita identificar directa o indirectamente al titular de los datos.
b) Implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado al riesgo, tales como la seudonimización y el cifrado.
c) Establecer procedimientos para verificar, evaluar y valorar regularmente la eficacia de las medidas técnicas y organizativas implementadas para garantizar la seguridad del tratamiento.
d) Designar un responsable del tratamiento de datos personales encargado de supervisar el cumplimiento de la presente normativa.

Artículo 21.- Procedimiento para la anonimización.- Las entidades financieras podrán seguir el siguiente procedimiento para la anonimización de datos personales de consumidores financieros:

a) Identificar los datos personales que serán objeto de anonimización.
b) Eliminar cualquier información que permita identificar directa o indirectamente al titular de los datos.
c) Implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado al riesgo.
d) Verificar, evaluar y valorar regularmente la eficacia de las medidas técnicas y organizativas implementadas.

e) Documentar el proceso de anonimización y conservar los registros correspondientes.

Sin perjuicio de lo indicado, los responsables podrán incorporar procedimientos propios o complementarios, en los que se deberá aplicar este procedimiento, sumado a los lineamientos que se añadan, sin que limiten el ejercicio de derechos de los titulares.

Artículo 22.- Excepciones. - La presente normativa no será aplicable en los siguientes casos:

a) Cuando los datos personales hayan sido previamente anonimizados por el titular de los datos.
b) Cuando los datos personales sean necesarios para el cumplimiento de una obligación legal o contractual.
c) Cuando los datos personales sean necesarios para la protección de intereses vitales del titular o de otra persona natural.

Artículo 23.- Falta grave. - Sera considerada una falta grave, la reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los clientes financieros.

Estarán exentos de la sanción cuando la reversión se deba a disposición de Autoridades Judiciales, Constitucionales, Servicio de Rentas Internas o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento.

DISPOSICIÓN TRANSITORIA

ÚNICA. - Las entidades que conforman el Sistema Financiero Nacional, en un plazo de ciento veinte (120) días, acoplarán sus políticas a lo establecido en la presente normativa.

DISPOSICIÓN FINAL

Esta normativa entrará en vigor a partir de su publicación en el Registro Oficial.

Dado en Quito, a los 10 días del mes de junio de 2024.

Dr. Fabrizio Roberto Peralta Díaz
SUPERINTENDENTE
SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES

Anexo II

MANUAL PARA EL TRATAMIENTO DE DATOS PERSONALES EN CONSUMIDORES FINANCIEROS, RESPECTO ELIMINACION, BLOQUEO Y ANONIMIZACION DE DATOS PERSONALES

VERSIÓN JUNIO 2024

Documentación de Procesos	
Tipo de Proceso	Estratégico.
Macroproceso	Gestión de Información de Clientes
Proceso	Todos los procesos.
Subproceso	Administración de datos personales
Alcance	Inicio: Desde la recopilación de la información de consumidores financieros.
	Fin: Conservación y/o eliminación de la información de consumidores financieros.
Objetivo	Detallar la gestión y controles a realizar en los procesos internos de la entidad financiera, para asegurar un manejo en el ciclo de vida de datos de los consumidores financieros, bajos los lineamientos de la Ley Orgánica de Protección de Datos Personales y demás normativas aplicables.
Producto o Servicio	Todos los productos y servicios de la entidad financiera.
Tipo de Cliente	Cliente Externo e Interno.
Nivel de Clasificación	Documento Interno

GLOSARIO DE TÉRMINOS

	Palabra	Definición
1	**Anonimización**	"Aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados" (LOPDP, Art. 4).
2	**Bloqueo**	"Identificación y reserva de los datos personales, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización" (Ley Orgánica 3/2018, Art. 32)
3	**Consentimiento**	Manifestación de la voluntad libre, específica, informada e inequívoca, por la que el titular de los datos personales/cliente o consumidor financiero) autoriza al responsable del tratamiento de los datos personales (entidad financiera) a tratarlos mediante cualquier medio idóneo, físico o electrónico.
4	**Ciclo de vida de datos**	Se refiere a la secuencia de etapas por las que atraviesan los datos personales a lo largo de su vida útil, desde el momento en el que se recopilan/obtienen, clasifican, almacenan, utilizan, modifican de ser el caso, y eliminan los datos
5	**Cliente Interno**	Accionistas, directores y/o colaboradores dentro de la empresa que toman el resultado o el producto de una actividad en un proceso como insumo para realizar actividades inherentes a su cargo. De la misma manera el resultado de su gestión será el insumo para la ejecución de otro proceso.

6	**Confidencialidad**	Se refiere al resguardo, no divulgación y protección de información y datos personales, determinados como no públicos por parte de la entidad financiera.
7	**Consumidor financiero**	Personas naturales que mantienen una relación contractual o utilizan los productos y servicios que ofrece la entidad financiera.
8	**Datos de consumidores financieros**	Toda información que para el presente documento refiere a personas naturales (datos personales), que los identifica o hace identificables, en particular mediante un identificador, nombre, número de identificación, datos de localización, o elementos propios de su identidad como los datos biométricos, salud, crediticios u otros determinados por la normativa vigente aplicable.
9	**Datos públicos**	Datos de personas naturales o jurídicas alojadas en fuentes de acceso público legitimas.
10	**Datos sensibles**	Es una categoría especial de dato personal que afecta la intimidad del Titular y cuyo uso inadecuado puede generar discriminación. Dichos datos consisten en información personal respecto etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales. Para efectos

		este documento, los datos sensibles aquí enunciados no se encuentran dentro de los datos de los consumidores financieros, toda vez que no son recopilados ni tratados por la entidad financiera
11	**Delegado de protección de datos**	Persona natural o jurídica, encargada de informar al responsable del tratamiento sobre sus obligaciones sobre protección de datos, supervisando el cumplimiento normativo en la materia.
12	**Eliminación de datos personales**	Es la eliminación total o parcial de la información personal del consumidor financiero en los repositorios, archivos, ficheros o tratamientos realizados por la entidad financiera.
13	**Encargado del tratamiento de datos**	Persona natural o jurídica, pública o privada, autoridad, u otro organismo que solo o juntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales. Está a cargo del cumplir con las políticas y directrices de tratamiento de datos de los consumidores financieros, dispuestas por el responsable de protección de datos.
14	**Organismo de Control**	Entidades facultadas a controlar el cumplimiento de normativas internas o externas a la entidad financiera.
15	**Privacidad**	Se refiere a la protección de todos los datos de los consumidores financieros contra el mal uso o la divulgación no autorizada de los mismos. La privacidad de datos no es aplicable a los reportes

		que realiza la entidad financiera por mandato normativo, y a los casos en los que una autoridad competente realiza requerimientos de información
16	**Protección de datos**	Conjunto de medidas técnicas y organizativas para garantizar y proteger los datos personales cuya custodia se encuentre en la entidad financiera, y son susceptibles de tratamiento.
17	**Recopilación**	Acción de recolectar datos
18	**Responsable del tratamiento de datos**	Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o junto con otros decide sobre la finalidad y el tratamiento de datos personales.
19	**Tratamiento de datos personales**	Cualquier operación o conjunto de operaciones realizadas sobre datos personales, mediante procesos automatizados, o manuales, que van desde la recopilación, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, distribución, cesión, comunicación o transferencia, supresión, destrucción y, demás usos de datos personales.

Procedimiento para el tratamiento de datos personales de consumidores financieros y eliminación de datos personales:

Antecedentes

Actualmente, la protección de datos personales es fundamental, por lo que implica su recopilación y tratamiento. A lo largo de la última década, la protección de datos ha sido tema de discusión y su regulación ha tomado una relevancia importante.

La Constitución de la República establece en su artículo 66 numeral 19 que garantizará a las personas el derecho a la protección de datos personales, que incluye el acceso y la decisión sobre información y datos de este carácter y su protección correspondiente. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

El Código Orgánico Monetario y Financiero dispone en su artículo 352 que los datos personales de los usuarios del sistema financiero nacional que reposan en las entidades y su acceso están protegidos, y solo podrán entregarse a su titular o a quien este autorice o dispongan este Código.

Por su parte, la Resolución No. SB-2020-540 de 21 de mayo de 2020, publicada en el Registro Oficial Suplemento 614, de 10 de enero del 2022, dispuso que cada entidad controlada que reúne recibe, posee, almacena, trata o maneja datos no públicos de los consumidores financieros, debe contar con políticas y procedimientos adecuados que aseguren que las prácticas y procedimientos de seguridad razonables para proteger los datos no públicos de los consumidores financieros, entre otros. Dentro de las definiciones de esta norma, el consumidor financiero puede ser una persona natural o jurídica.

Cabe destacar la necesidad de la entidad financiera de tener un proceso documentado para la protección de la información, enfocada en los datos de los consumidores financieros, para garantizar que se cumpla la normativa vigente en sus procesos internos y los derechos de estos, y según creyere conveniente, la

adopción de manuales para la administración de la información personal de sus consumidores financieros y clientes.

CONSIDERACIONES GENERALES

El presente documento se fundamenta en los siguientes Principios Generales que son de aplicación directa:

Propiedad: Los consumidores financieros son los propietarios de los datos personales que la entidad financiera recopila, en los términos aquí establecidos.

Lealtad: El tratamiento de datos siempre será leal, en la prestación de servicios y/o entrega de productos dentro del giro del negocio de la entidad financiera.

Finalidad de los datos: Los datos recopilados deben tener un fin específico y definido, para usos legítimos relacionados exclusivamente al objeto social de la entidad financiera y los productos y servicios que contraten o usen los consumidores financieros, o mejoramiento de estos. Además del cumplimiento irrestricto de las normas de sigilo y reserva bancaria, está prohibido para todos los colaboradores de la entidad financiera acceder y usar los datos con fines distintos y ajenos a sus funciones laborales. Esto incluye los datos en cualquier formato y en cualquier ubicación.

Ciclo de datos: Se debe asegurar que el proceso para la administración de datos está de acuerdo con el ciclo de vida de gestión de datos. El responsable de datos debe garantizar procedimientos apropiados con el objeto de mantener la calidad e integridad de los datos que tienen acceso.

Actualización de la información: Los registros de datos deben mantenerse actualizados en todas las etapas del flujo de trabajo y de una manera auditable y trazable. Para este fin, la entidad financiera implementa procesos de actualización en los registros de datos.

Medidas de seguridad en formato electrónico: Los datos almacenados en un formato electrónico siempre deben ser protegidos por salvaguardas apropiadas en electrónicos y/o controles de acceso físico que restringen el acceso sólo para usuarios autorizados.

Seguridad de datos: El órgano interno de la entidad financiera, encargado de la gestión y administración de información de clientes, deberá implementar todas las medidas de seguridad adecuadas y necesarias, sean éstas organizativas, técnicas o de cualquier otra índole, para proteger los datos frente a cualquier riesgo, amenaza y vulnerabilidad.

Conservación: Los datos se conservarán durante un tiempo menor al necesario para cumplir con el fin de su tratamiento, según el producto o servicio contratado y a lo que establezca la normativa vigente.

Todos los datos que se encuentren bajo custodia de la entidad financiera serán tratados de acuerdo con las categorías de datos personales, determinadas por la Ley Orgánica de Protección de Datos Personales, su reglamento de Aplicación, así como la Política de Seguridad de la Información y a los demás documentos que se expidan para el efecto.

Eliminación, anonimización y bloqueo de datos personales:

Después de cumplido el plazo o condiciones que determina la normativa vigente aplicable, el banco como responsable del tratamiento deberá aplicar los mecanismos necesarios para anonimizar o bloquear datos personales, adoptando las medidas razonables para que se efectúen estos procesos.

Derecho de eliminación: El titular tiene derecho a que el responsable del tratamiento elimine, bloquee o anonimice sus datos personales, cuando:

1. El tratamiento no cumpla con los principios establecidos en la presente ley;
2. El tratamiento no sea necesario o pertinente;

3. Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;
4. Haya vencido el plazo de conservación de los datos personales;
5. El tratamiento afecte derechos fundamentales o libertades individuales;
6. Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o,
7. Exista obligación legal.

Asimismo, conforme determina el Reglamento de aplicación a la Ley Orgánica de Protección de Datos Personales, se podrán bloquear o anonimizar datos personales cuando se cumpla las finalidades de su tratamiento y ya no exista necesidad de mantenerlos en uso, lo cual puede involucrar la petición expresa del cliente o consumidor financiero.

El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a anonimizar hacer ilegible, o dejar irreconocibles de forma definitiva y segura los datos personales. Esta obligación la deberá cumplir en el plazo de quince (15) días de recibida la solicitud por parte del titular y será gratuito.

Cuando proceda la efectivización de este proceso, se notificará al titular mediante de forma escrita y motivada, sea mediante la aceptación a su solicitud, como su negativa, según sea aplicable.

A los efectos de que, se proceda a anonimizar o bloquear los datos solicitados por parte del titular; se seguirá el procedimiento que se describe a continuación:

- Se procederá a la eliminación física de los datos de carácter personal:
    - Respecto de los datos contenidos en soporte papel, el proceso a realizar podrá tener lugar mediante la destrucción física del

documento, siguiendo el procedimiento descrito en el correspondiente manual de Plazos de Conservación.

- Si los datos están contenidos en soporte informático, se realizará este proceso sin que sea suficiente el empleo de una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las cancelaciones.

- Sin perjuicio de lo anterior, cuando sea necesaria la conservación de los datos, por alguno de los siguientes motivos:

  - Porque pudieran derivarse responsabilidades,
  - Pueda causar un perjuicio a intereses legítimos del titular de los datos o de terceros.
  - Una norma imponga la obligación de conservar los datos durante un periodo determinado.
  - Los datos y documentación sirvan como justificante de una actividad o servicio prestado, durante los plazos de prescripción de las acciones civiles, penales, administrativas o de cualquier otro tipo que pudieran derivarse de la actividad o servicio prestado.

Se procederá a minimizar los datos necesarios a conservar; Anonimizar o seudonimizar la información de ser posible y bloquear la misma para evitar que pueda existir un acceso a los datos salvo por aquellas personas que lo requieran por los motivos que se justifican en las causas de conservación.

Consideraciones importantes:

a. Cuando el titular de los datos personales requiera solicitar el ejercicio del derecho de eliminación o anonimización de datos personales, el Banco luego de recibirla y evaluar la pertinencia de dicho requerimiento, deberá bloquear

los datos objeto de este proceso como medida preventiva, y una vez concluida su idoneidad deberá proceder a la anonimización.

El proceso de bloqueo será el mismo al utilizado respecto mecanismos seguros en cuentas bancarias, inversiones, tarjetas de crédito y demás servicios o productos financieros; es decir, cuando exista requerimiento expreso del cliente, por solicitud de autoridad competente o cuando exista obligación legal de realizarla. Para ello se deben poner en práctica los procedimientos que demanda la Norma de control para la gestión del riesgo operativo para las entidades financieras (normativa especializada).

b. En este sentido, para la correcta anonimización de datos personales, cuando la finalidad implique la no identificación del titular o sus datos que lo hagan identificable, de tal manera que ya no sea posible re identificarlo, se usarán mecanismos de seudonimización, agregación de datos. Para la anonimización de datos relativos a cuentas bancarias, tarjetas de crédito o productos financieros que contengan una identificación especifica, el mecanismo a utilizarse será el enmascaramiento de datos. Por otro lado, para la anonimización de datos de identificación directa del consumidor financiero (como numero de cedula, pasaporte o DNI), se podrá utilizar la tokenización.

En todo caso se observarán los plazos de conservación establecidos en el Procedimiento de Plazos de Conservación; y, una vez finalizado dicho plazo se procederá a la supresión de la información en los términos aquí previstos; y/o a la anonimización de la misma, en caso de requerirse la conservación de información no personal.

REGISTRO DE ELABORACIÓN/ ACTUALIZACIÓN

Registro de Elaboración/ Actualización			
Versión	**Fecha**	**Hecho por**	**Referencias de Cambio**
2			
1			

Anexo III

ENTREVISTAS A FUNCIONARIOS DE ENTIDAD BANCARIA

Entrevistador: David Ayala Carrasco y Christian Portero

Fecha de la entrevista: 26 mayo 2024

20h00.

David Ayala: Como parte del trabajo de investigación denominado "Aplicación del bloqueo o anonimización de datos personales en consumidores bancarios, como parte del derecho de eliminación determinado en la normativa en materia de protección de datos personales en el Ecuador, se ha previsto realizar una serie de entrevistas a funcionarios de entidades bancarias domiciliadas en Quito con conocimientos en derecho y protección de datos, con el fin de conocer sus criterios y opiniones sobre la temática, de manera cualitativa, por lo que empezaremos con las preguntas.

PREGUNTA 1

Entrevistador

La apertura del de la entrevista la realizamos con una pregunta bastante general y bueno, antes de nada, la forma de conversación será que nosotros realizamos la consulta, y cualquiera de ustedes puede sentirse libre de contestarla ya la idea es que con cada pregunta los tengamos la retroalimentación de su parte.

En este sentido, la primera pregunta es ¿***cuál es su opinión sobre la importancia de la Protección de Datos personales en el sector financiero***?

Entrevistado No. 1

A ver, a mi modo de ver el sector bancario es uno de los sectores que más cantidad y variedad de datos personales maneja.

Los clientes entregan voluntariamente al Banco mucha información de tipo económica, estatus de empleo, ingresos, gastos, presupuesto económico en

general y aún más importante, quizás sobre sí mismos. Datos sobre incluso sobre sus familias, por aquello de tener que observar incluso leyes sobre prevención de lavado de activos. Entonces, las instituciones bancarias, al contar con una base de datos, digamos tan amplia por el número de clientes que tiene, así como por el número de Datos a los que tiene acceso, es fundamental el correcto manejo de estos datos personales. Por lo explicado, son los clientes, se les le entregan voluntariamente variedad de Datos, por tanto, de necesariamente tiene que ser regulado ese tratamiento.

Entrevistado No. 2

Complementando tal vez un poco, creo que también es importante recapitular el impacto en la actualidad. O sea, si bien a lo largo de los años se ha venido realizando el tratamiento de los datos personales, no sé cuenta con una un tratamiento adecuado, y claro, ajustándonos ahora a la nueva realidad y a la implementación de GDPR en la Comunidad Europea y aquí en El País, la Ley Orgánica, creo que es justamente el hito o el inicio de darle un buen y un justo tratamiento a los datos personales de las personas, sobre todo tomando en cuenta que se trata de categorías especiales y por el impacto que puede tener justamente que no haya el debido control o que se pueda esparcir o velar, es información que al final del día es prácticamente el uso diario de las personas y de sus relaciones personales. Económicos.

PREGUNTA 2.

Entrevistador

Claro, lógicamente, en este sentido es preciso también arribar a una pregunta más específica sobre ***los riesgos que ustedes creen puedan enfrentar las entidades financieras, al aplicar los lineamientos generales o subjetivos de la norma, de manera incorrecta.***

Entrevistado No. 1

Sin duda deben implementar políticas, manuales de procesos, guías de tratamiento, pues la información que las entidades bancarias han accedido desde antes de la ley, ha sido manejada con restricciones basadas a seguridad de la información y no tanto a privacidad de datos, lo cual tenía muchos resultados, desde cosas menores, como lo molesto que era recibir llamadas de telemarketing, de productos que uno nunca había solicitado, hasta temas más graves, como estafas, robos de identidad debido a la falta de seguridad en el manejo de los datos. Ahora, en hay que tomar en cuenta también el desarrollo de la tecnología, que es muy rápido, pero a la cual nosotros queremos que la mayoría de las personas económicamente activas se unan, que sean bancarizadas, entonces quiere decir que hay un manejo de un manejo de Datos bases físicas, sino también hay un mayor riesgo intangible, de la información que ya no está almacenada físicamente y que, quizás necesitaba de otro tipo de medidas de seguridad, pero hoy en día, con la tecnología existe este riesgo también de que toda esta información sea manejada y no sea mal habida por personas inescrupulosas, por delincuentes que bien pueden estar aquí, junto a nosotros como pueden estar al otro lado del del planeta. Entonces, ahí hay varias aristas de en relación con la privacidad de los datos que deben tener en cuenta las entidades bancarias.

Entrevistado No. 2

Correcto y creo que también es importante considerar que existen dos factores determinantes, uno es el personal de los del sector bancario qué tratan información y esto más en el sentido de qué tan capacitados están en este aspecto, Qué personas tienen o no el acceso, y lo peligroso que es que las personas no conozcan de las normas desde lo más básico, como por ejemplo mantener su computador desbloqueado, mantener la información ahí a la periferia y a la mano de cualquier

persona, y el otro que creo que viene a ser también el aspecto más importante que mencionó vane, que es la tecnología.

PREGUNTA 3.

Entrevistador

Claro, y desde que ustedes comentan, ahí yo creería que tal vez hay otro punto que es bueno considerar, y va en forma de pregunta, pero va encaminado también a cómo regula la autoridad en la materia, y en este punto también arriba la pregunta: ***¿ustedes sienten como como titulares de Datos a sí mismo como colaboradoras en entidades financieras, que es necesario exista una normativa específica sobre el punto central, que es anonimizar o bloquear datos personales?*** entendiendo la anonimización como el proceso en el que un dato deja de identificarme es decir, mi dato como como "*Juanito Pérez*", ya no puede estar asociado a ningún otro dato, y eso de alguna manera precautela la integridad y garantía de mi derecho.
¿Pero ustedes creen que es necesario que exista una resolución, un proyecto de resolución o creen que tal vez con las normas que se han expedido es más que suficiente?

Entrevistado No. 2

En lo personal no creo que estemos en capacidad con la ley que tenemos actualmente de afrontar que este tipo de aspectos, porque básicamente y con todo el respeto, se trata más meramente de una copia. Entonces, no creo que necesariamente los artículos del detalle en el que nos estamos basando se ajusta a las necesidades reales y específicas de la realidad de este país.
Porque tal vez una resolución o un proyecto creo que va más allá de ponerlo en papel, ponerlo en la práctica y eso no serviría justamente para poder medir en qué nivel está, no solo el sector bancario, sino en general las compañías no y las

personas que hacen el tratamiento de Datos de qué manera en realidad se está aplicando, porque básicamente se tuvo un tiempo de implementación, digamos, para ver cómo funcionaba o que riesgos y medidas se adoptaban, pero en la realidad, qué tanto se profundizó y se aplicó desbloqueado, y el segundo factor que es la tecnología, y digamos, especializado, el tema no solo para dar un neto cumplimiento, sino en realidad para darle la atención que amerita, no?

Entrevistado No. 1

Sí, en parte estoy de acuerdo, sin embargo, dado que la ley misma establece que la administración es una de las medidas que los responsables pueden incluir para lograr la seguridad de los datos que tratan en se tendría que ir de la mano con regulaciones de otros métodos, pero yo creo que ayudaría. Pienso que las instituciones al momento si han tratado de establecer procesos y medidas a su mejor criterio.

Sin embargo, una guía de cómo realizar las cosas tanto en la parte operativa y teórica, quizás otorgándole al órgano de control un poder de auditoría, pero no con fines sancionatorios, sino más para para que sea una verdadera guía para lograr el fin de la ley, que no es sancionar, sino proteger los datos de los titulares.

Creo que sí puede ayudar, solo que, en efecto, no sé qué tan qué tan efectiva puede ser, dado que el resto de la ley no existen todavía directrices respecto de la aplicación de esta, o sea, existe el Reglamento, pero hay mucho, mucho que falta por desarrollar, modelos que la autoridad debería implementar, procesos que la autoridad debería implementar desde ahorita, porque falta incluso calificar a los delegados de Protección de Datos de los responsables de las empresas, entonces falta mucho por hacer, sin embargo, sí pienso que a largo plazo esto podría ayudar a una mejor regulación y para llegar al fin de la ley, como digo, es que es la protección adecuada de los datos.

PREGUNTA 4.

Entrevistador

¿Claro, Y justo esa es una de las de las tareas de la Autoridad de Protección de Datos, sin embargo, como ustedes ven ya la norma establece sanciones por el incumplimiento de ciertos procesos que te que te dice como el de establecer medidas técnicas operativas y el ejercicio de derechos, ***¿Ustedes creen que exista hoy por hoy o en un futuro cercano Implicaciones legales drásticas para las entidades financieras sobre la falta de aplicación de los mecanismos de anonimización y bloqueo de datos personales, entendiendo que esta es una alternativa al derecho de eliminación?***

Entrevistado No. 1

Probablemente ahora me parece que el público está muy poco educado en relación a ejercer sus derechos sobre protección de sus datos, sin embargo, pensaría que con el tiempo esto poco a poco va a ir aumentando, la gente va a ir conociendo más, se educará un poco más, o al menos habrá una socialización mayor acerca de este tema y con ellos, sin duda crece el riesgo para las entidades financieras, tanto de enfrentar posibles sanciones de los organismos de control, así como de enfrentar posibles demandas.

Y la consecuente probabilidad de tener que pagar reparaciones de tipo económicas a los titulares de Datos en casos de violaciones de cualquier tipo de violaciones, entonces sí, sí, va a haber.

Entrevistado No. 2

Totalmente de acuerdo y creo que esto se trata también justo como dice de un tema cultural, de venir a educar a la sociedad a los ciudadanos y a los usuarios sobre la relevancia de sus datos, pero también sobre estos es el ejercicio de estos derechos que tienes no en la ley. No creo que estemos en ese nivel aún, creo que aún nos

falta un largo camino, pero sí creo que una vez que aparte de tener la autoridad se puedan desarrollar, digamos mesas de ayuda, mesas de información o incluso material que puedas encontrar en medios informáticos. Vas a poder conocer de qué manera ejercer esos derechos y creo que lo hemos visto, tal vez son muy pocos los casos de aquí en Ecuador, pero sí se han visto casos en los que justamente entra este malestar o esta molestia de por qué me llaman todo el tiempo a vender productos.

Yo no me suscribí porque tienen mi contacto en otro Banco X que sí creo que genera una preocupación, sobre todo con la situación de seguridad que vive El País y creo que ese también puede ser un impulso para que las personas empiecen a solicitar a los bancos o conocer también de qué manera se están tratando sus datos, creo que sí van a haber repercusiones legales y esperaría la verdad que las sanciones sí lleguen a ser altas, porque yo personalmente considero que es la única manera en la que le va a pesar sobre todo el Sector financiero cumplir de manera rígida con esta, con esta normativa.

PREGUNTA 5.

Entrevistador

Y para finalizar, esta pregunta más va desde el ponernos el sombrero de una entidad financiera y dentro de su desenvolvimiento que tienen en la en la institución, en la organización. ***¿Ustedes creen que el sistema financiero como tal, más allá de especificar un Banco a una cooperativa, está implementando medidas de anonimización adecuadas o tiene un nivel de madurez adecuado al respecto? ¿Y cuáles creen ustedes que serían al menos un mecanismo adecuado de anonimizar Datos?***

Entrevistado No. 2

Creo que básicamente no, lo primordial para mí viene a ser primero la evaluación de los riesgos y creo que en general aquí en el Ecuador no existe una buena evaluación de riesgos en el sentido de que si puede evaluar a qué riesgos estoy expuesto, pero con parámetros reales, o sea, con una matriz o una evaluación muy precisa.

Creo que puedo determinar cómo puedo prevenir y ver qué mecanismo es el más adecuado para cada institución, porque creo que todo depende también del nivel, digamos, volumen que tiene cada entidad, Banco o cooperativa, porque no siempre el target va a ser el mismo, y también creo que se basa mucho en dar esta seudonimización, porque si bien estamos diciendo que estamos volviendo la información no identificable, ¿de qué manera o con qué mecanismo le aseguramos nosotros a las personas que lo estamos haciendo?, porque una cosa es ponerlo escrito sobre papel, como se ha visto que sí se eliminará, o se destruirá la información, pero creo que va un poco más allá, saber en qué aspecto físico o visible, digámoslo vamos a realizar.

Entrevistado No. 1

Yo creo que a partir de que la ley fue emitida en el 2021 y que el Reglamento fuera emitido en el 2023, mucho más con este último, las instituciones bancarias han puesto énfasis en implementar medidas para brindar mayor seguridad a los datos, sin embargo, la falta de directrices por parte del órgano de control ante esa falta de directrices, cada institución ha implementado sus propios procesos bajo el mejor de sus criterios, es decir, subjetivamente. Esta implementación, sin embargo, de lo que podríamos llamar las mejores medidas posibles, en tanto no existen directrices.

Yo pienso que siempre va a existir un sesgo, una tendencia a preservar prácticas que pero que muy probablemente facilitaban o facilitan el desarrollo de los negocios o

hacen más fácil el conseguir al cliente, por tanto, siempre habrá una inclinación a encontrar vacíos o interpretar la norma a conveniencia de la institución, entonces creo que sí hace falta un poco más de directrices por parte del órgano de control en y una, o sea, una guía adecuada por parte del órgano de control.

Ojalá que las autoridades que fueron elegidas vengan con ese objetivo en la mira más que se han sido notorio, porque definitivamente todos estamos en un terreno no probado antes, entonces pienso que se está haciendo lo mejor posible en pocas palabras, pero muy probablemente no es suficiente, o sea, todavía vemos violaciones todavía y por un buen tiempo se van a ver violaciones por parte de las instituciones financieras, aunque todavía no ha habido sanciones. pero sabemos que existen y que bueno, lo que me preocupa a mí es que se vea una interpretación muy subjetiva de la norma.

Anexo IV

ESQUEMA ENCUESTA - ANONIMIZACIÓN O BLOQUEO DE DATOS PERSONALES

1. **¿Estás familiarizado con los conceptos de anonimización y bloqueo de datos personales?**

   SI

   NO

2. **¿Qué nivel de importancia le asignas a la anonimización de datos personales en el contexto legal ecuatoriano?**

   Muy importante

   Importante

   Neutral

   Poco importante

   Nada importante

3. **¿Conoces si en tu entidad bancaria se llevan a cabo procesos de anonimización de datos personales para proteger los datos personales de sus clientes?**

   SI

   NO

4. **¿Cuál es tu grado de confianza en la efectividad de las técnicas de anonimización y bloqueo de datos personales que aplican las entidades bancarias ecuatorianas?**

   Muy confiado

   Confiado

   Neutral

   Poco confiado

Nada confiado

5. **¿Crees que la regulación actual en Ecuador proporciona suficiente orientación sobre cómo llevar a cabo la anonimización y bloqueo de datos personales en el sector bancario?**

   Sí

   No

6. **¿Has encontrado desafíos específicos o dificultades al requerir a una entidad bancaria se anonimicen tus datos personales para su tratamiento?**

   Sí

   No

7. **¿Qué medidas adicionales crees que podrían ser necesarias para mejorar la protección de datos personales en las entidades bancarias en Ecuador?**

   Mayor supervisión por parte de entidades reguladoras

   Mejora de tecnologías de anonimización y bloqueo

   Capacitación adicional para el personal

   Otro:

8. **¿Cuál de las siguientes técnicas consideras más efectiva para la anonimización de datos en entidades bancarias?**

   Eliminación de identificadores directos (nombres, números de identificación)

   Encriptación de datos

   Agregación de datos

   Otro:

9. **¿Consideras necesaria una regulación específica relacionada con la anonimización y bloqueo de datos personales para las entidades bancarias?**

   Sí

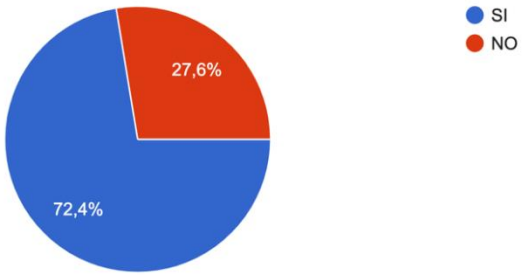
   No

Anexo V

TABULACIÓN RESULTADOS ENCUESTA

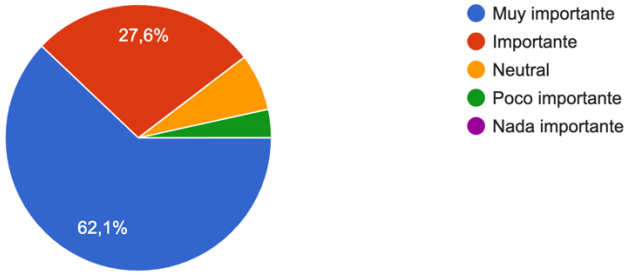
¿Estás familiarizado con los conceptos de anonimización y bloqueo de datos personales?

29 respuestas



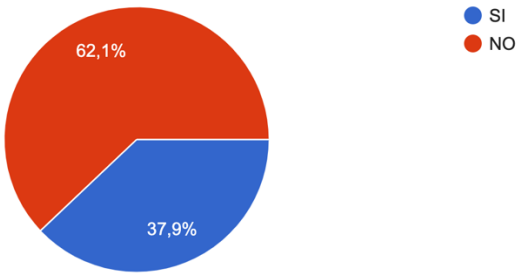
¿Qué nivel de importancia le asignas a la anonimización de datos personales en el contexto legal ecuatoriano?

29 respuestas



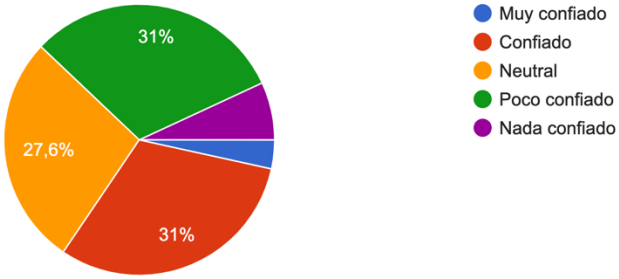
¿Conoces si en tu entidad bancaria se llevan a cabo procesos de anonimización de datos personales para proteger los datos personales de sus clientes?

29 respuestas



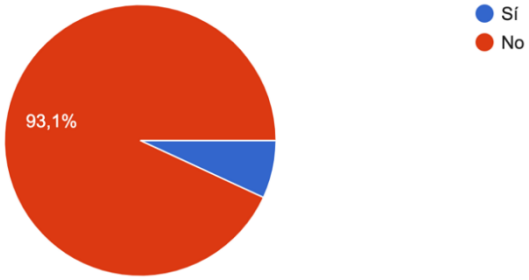
¿Cuál es tu grado de confianza en la efectividad de las técnicas de anonimización y bloqueo de datos personales que aplican las entidades bancarias ecuatorianas?

29 respuestas



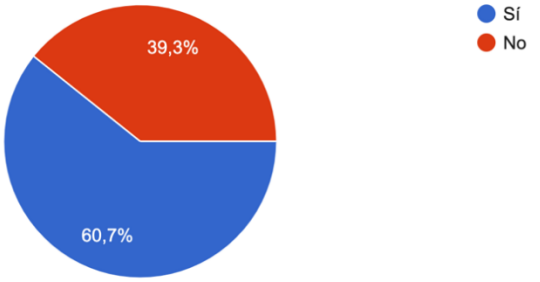
¿Crees que la regulación actual en Ecuador proporciona suficiente orientación sobre cómo llevar a cabo la anonimización y bloqueo de datos personales en el sector bancario?

29 respuestas



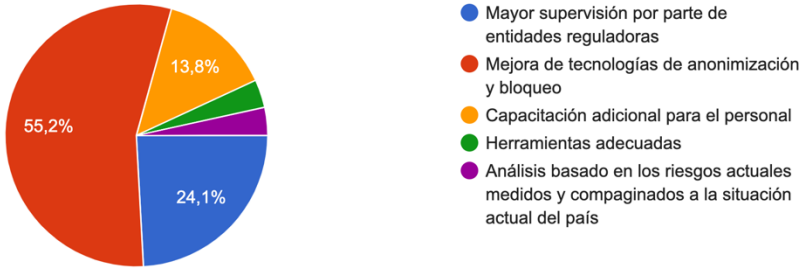
¿Has encontrado desafíos específicos o dificultades al requerir a una entidad bancaria se anonimicen tus datos personales para su tratamiento?

28 respuestas



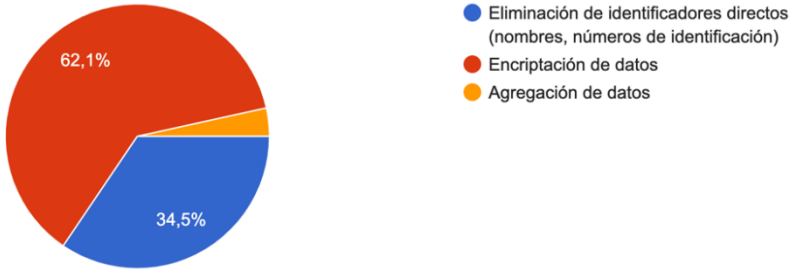
¿Qué medidas adicionales crees que podrían ser necesarias para mejorar la protección de datos personales en las entidades bancarias en Ecuador?

29 respuestas



¿Cuál de las siguientes técnicas consideras más efectiva para la anonimización de datos en entidades bancarias?

29 respuestas



¿Consideras necesaria una regulación específica relacionada con la anonimización y bloqueo de datos personales para las entidades bancarias?

29 respuestas