UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TEMA:

Efectos del uso indebido de datos personales en la gestión extrajudicial de cobranza

AUTORES:

Pico Trujillo Iván Rafael

Estupiñán Cervantes José René

Trabajo de titulación previo a la obtención del grado de

ABOGADO

TUTOR:

Dr. Marco Antonio Elizalde Jalil, PhD.

Guayaquil, Ecuador

20 de febrero del 2025

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **IVÁN RAFAEL PICO TRUJILLO Y JOSÉ RENÉ ESTUPIÑÁN CERVANTES**, como requerimiento para la obtención del Título de **Abogado.**

TUTOR

f. _____
Dr. Marco Antonio Elizalde Jalil, PhD.

DIRECTORA DE LA CARRERA

f. _____
Dra. Nuria Pérez Puig-Mir, PhD.

Guayaquil, a los 20 días del mes de febrero del año 2025

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, **PICO TRUJILLO IVÁN RAFAEL y ESTUPIÑÁN CERVANTES JOSÉ RENÉ**

DECLARAMOS QUE:

El Trabajo de Titulación, **EFECTOS DEL USO INDEBIDO DE DATOS PERSONALES EN LA GESTIÓN EXTRAJUDICIAL DE COBRANZA,** previo a la obtención del Título de **Abogado**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 20 días del mes de febrero del año 2025

LOS AUTORES

f. _____
PICO TRUJILLO IVÁN RAFAEL

f. _____
ESTUPIÑÁN CERVANTES JOSÉ RENÉ

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

AUTORIZACIÓN

NOSOTROS, PICO TRUJILLO IVÁN Y ESTUPIÑÁN CERVANTES JOSÉ

Autorizamos a la Universidad Católica de Santiago de Guayaquil a la publicación en la biblioteca de la institución del Trabajo de Titulación, **EFECTOS DEL USO INDEBIDO DE DATOS PERSONALES EN LA GESTIÓN EXTRAJUDICIAL DE COBRANZA**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 20 días del mes de febrero del año 2025

LOS AUTORES:

f. _____
PICO TRUJILLO IVÁN RAFAEL

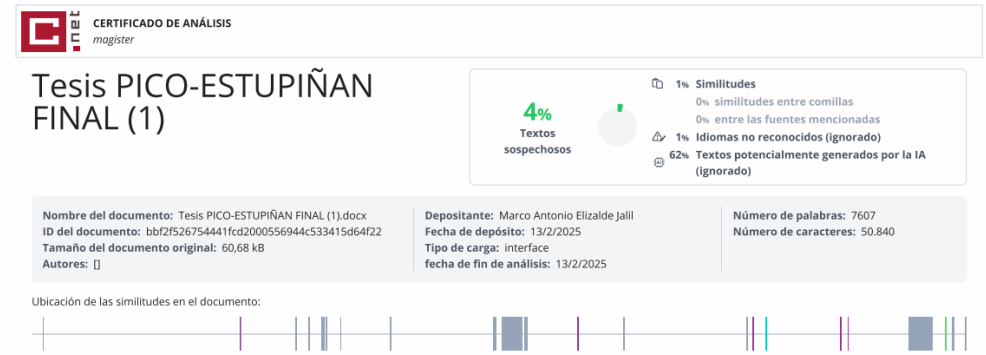
f. _____
ESTUPIÑÁN CERVANTES JOSÉ RENÉ

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

REPORTE DE COMPILATIO


CERTIFICADO DE ANÁLISIS
magister

Tesis PICO-ESTUPIÑAN FINAL (1)

4% Textos sospechosos

1% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
1% Idiomas no reconocidos (ignorado)
62% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: Tesis PICO-ESTUPIÑAN FINAL (1).docx
ID del documento: bbf2f526754441fcd2000556944c533415d64f22
Tamaño del documento original: 60,68 kB
Autores: []

Depositante: Marco Antonio Elizalde Jalil
Fecha de depósito: 13/2/2025
Tipo de carga: interface
fecha de fin de análisis: 13/2/2025

Número de palabras: 7607
Número de caracteres: 50.840

Ubicación de las similitudes en el documento:

Guayaquil, a los 20 días del mes de febrero del 2025.

Autores

f. _____
PICO TRUJILLO IVÁN RAFAEL

f. _____
ESTUPIÑÁN CERVANTES JOSÉ RENÉ

Tutor

f. _____
DR. ELIZALDE JALIL, MARCO ANTONIO, Ph

AGRADECIMIENTO

Quiero agradecer a las personas que han estado conmigo en cada paso de este largo camino. A mis padres, que fueron fuente de inspiración y resiliencia. Nunca me dejaron caer y me ayudaron a llegar a donde estoy. A mi compañera fiel que se mantuvo a mi lado en los momentos difíciles y fue mi apoyo incondicional. Gracias por creer en mí y ayudarme a llegar hasta aquí. De igual manera, agradecer a mis estimados docentes, quienes fueron guías y verdaderos maestros, fuentes de inspiración de lo que significa esta carrera y esta honorable profesión.

Iván Rafael Pico Trujillo.

Quiero agradecer principalmente a mis padres, quienes han sido mi sostén e incondicional apoyo a lo largo de estos años de carrera. A mis amigos, docentes y experiencias que he sumado, que me han hecho quien soy y me han ayudado a formarme. De igual manera agradecerle a mi compañero de tesis, Iván, quien fue uno de mis primeros amigos en la universidad y me ha ayudado a crecer a lo largo del camino.

José René Estupiñán Cervantes.

DEDICATORIA

Quiero dedicar este trabajo a mis padres, a mis abuelas que desde el cielo me cuidan y me apoyan, aunque físicamente no estén aquí conmigo, las llevo siempre en el corazón y en mis pensamientos. De igual manera, dedicar este trabajo a mi fiel compañera, Belén, por ser mi luz y ayudarme a llegar a donde estoy.

Iván Rafael Pico Trujillo

Dedico este trabajo a mis queridos padres, a mis primos, a mi familia, a mi ciudad natal, quienes me han formado en carácter. De igual manera, quiero dedicar este trabajo a mis amigos cercanos que han sido un apoyo incondicional a lo largo de este trabajo, inspirando y motivándome a seguir adelante. Por último, a Dios, que ha sido mi guía y mi luz durante tiempos de oscuridad.

José René Estupiñán Cervantes.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

_____

Abg. Elker Paulova Mendoza Colamarco

Oponente

_____

Dr. Leopoldo Xavier Zavala Egas

Decano

_____

Abg. Maritza Reynoso de Wright, Mgs.

Coordinadora de Unidad de Titulación

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Facultad: **Jurisprudencia**

Carrera: **Derecho**

Período: **UTE SEMESTRE B-2024**

Fecha: 20 de febrero de 2025

ACTA DE INFORME FINAL

El abajo firmante, docente tutor del Trabajo de Titulación denominado **"EFECTOS DEL USO INDEBIDO DE DATOS PERSONALES EN LA GESTION EXTRAJUDICIAL DE COBRANZA"** elaborado por los estudiantes **PICO TRUJILLO IVÁN Y ESTUPIÑÁN CERVANTES JOSÉ**, certifica que durante el proceso de acompañamiento dichos estudiantes han obtenido la calificación de **8 (ocho)**, lo cual la califica como APTA PARA LA SUSTENTACIÓN.

Dr. Marco Antonio Elizalde Jalil, PhD.

ÍNDICE GENERAL

RESUMEN

El uso indebido de datos personales en la gestión extrajudicial de cobranza vulnera el derecho a la privacidad, generando un conflicto entre la recuperación de deudas y la protección de los derechos de los deudores. Las empresas, al implementar tecnologías de análisis de datos para optimizar la cobranza, pueden incurrir en prácticas invasivas, como llamadas frecuentes, mensajes en horarios inoportunos o el rastreo digital, lo cual afecta la privacidad de los individuos. Este escenario plantea dilemas éticos y legales sobre la proporción de las medidas adoptadas, y hasta qué punto el uso de estos datos está justificado sin afectar la intimidad del deudor. En el presente trabajo se pretende abordar como el uso indebido de datos personales vulnera el derecho a la privacidad en la gestión de cobranza de las empresas, ya que se ha vuelto fundamental en el contexto actual, marcado por la digitalización y la expansión de las tecnologías de información. Si bien estas herramientas permiten a las organizaciones mejorar sus procesos de recuperación de deudas, también generan preocupaciones significativas sobre la privacidad de los individuos. Este estudio examina cómo las prácticas de gestión de cobranza impactan el derecho a la intimidad de los deudores, abordando temas como la recopilación y almacenamiento de datos personales, el uso de tecnologías avanzadas para localizar deudores y la comunicación a través de diversos canales que pueden resultar invasivos.

Palabras clave: Datos personales, Gestión de cobranza, Derecho a la privacidad, Efectos jurídicos, Abuso

ABSTRACT

The improper use of personal data in extrajudicial collection management violates the right to privacy, generating a conflict between debt recovery and the protection of debtors' rights. Companies, when implementing data analysis technologies to optimize debt collection, may engage in invasive practices, such as frequent calls, messages at inopportune times or digital tracking, which affects the privacy of individuals. This scenario raises ethical and legal dilemmas about the proportion of the measures adopted, and to what extent the use of this data is justified without affecting the debtor's privacy. This paper aims to address how the misuse of personal data violates the right to privacy in the collection management of companies, as it has become fundamental in the current context, marked by digitization and the expansion of information technologies. While these tools enable organizations to improve their debt recovery processes, they also raise significant privacy concerns for individuals. This study examines how collection management practices impact debtors' right to privacy, addressing issues such as the collection and storage of personal data, the use of advanced technologies to locate debtors, and communication through various channels that can be invasive.

Keywords: Personal data, Collection management, Right to privacy, Legal effects, Abuse, Privacy rights

INTRODUCCIÓN

Según (Wilkins, 2018) “La cobranza extrajudicial se refiere a todas las gestiones, acciones o trámites que realiza un acreedor de manera no judicial con el objetivo de lograr que un deudor moroso cumpla con sus obligaciones”.

La gestión extrajudicial de cobranza ha adquirido una relevancia significativa en el contexto actual, especialmente por el aumento de las prácticas abusivas que afectan a los consumidores. En este marco, es fundamental que las actuaciones de cobranza, independientemente de su naturaleza o medio de comunicación, se alineen con principios éticos y legales que garanticen el respeto a la dignidad y a la integridad de los deudores (Revista Progreso, 2021). Estos principios incluyen la proporcionalidad, razonabilidad, justificación, transparencia, y el respeto a la privacidad del hogar del consumidor.

La normativa vigente establece que no se cumple con estos principios cuando, por ejemplo, un proveedor de crédito o una empresa de cobranza realiza más de un contacto telefónico o visita por semana. Asimismo, se prohíbe llevar a cabo más de dos gestiones semanales a través de correspondencia, mensajes de texto o correos electrónicos, debiendo existir un intervalo mínimo de dos días entre cada gestión. Estas regulaciones buscan prevenir el hostigamiento y proteger la salud mental del consumidor, evitando así prácticas que puedan resultar intimidatorias o invasivas (Barocelli, 2020).

Además, las empresas encargadas de la cobranza extrajudicial tienen la obligación de informar al deudor sobre los medios de contacto disponibles y registrar la frecuencia y tipo de gestiones realizadas. Este registro debe ser mantenido por un período mínimo de dos años, lo que proporciona un marco para la rendición de cuentas y transparencia en las acciones llevadas a cabo (Wilkins, 2018).

Sin embargo, el uso indebido de datos personales en este contexto puede acarrear consecuencias graves. La falta de cumplimiento con las normativas sobre protección de datos puede llevar a sanciones significativas para las empresas involucradas. Esto incluye no solo multas económicas, sino también daños a la reputación y confianza del consumidor. La gestión inadecuada de información personal puede resultar en violaciones a los derechos fundamentales, generando situaciones donde los consumidores son contactados sin justificación o son objeto de amenazas y acosos.

CAPÍTULO I

1.1. RÉGIMEN JURÍDICO DE LOS DATOS PERSONALES

Según el tratadista Oscar Puccinelli, define el concepto de dato lo define como un elemento específico y aislado que, por sí mismo, no constituye una información completa. Para que un dato se convierta en información, es necesario establecer conexiones entre estos elementos, de modo que, al relacionarse, produzcan una referencia concreta y significativa. Así, la transformación de datos en información implica la habilidad de contextualizar, vincular y otorgar significado a estos elementos aislados, lo que permite crear una representación más integral y comprensible de la realidad (Puccinelli, 1999).

Por otra parte, la Real Academia Española define El término "dato", en su comprensión actual, proviene de la palabra latina "datum", que se traduce como "antecedente necesario para alcanzar un conocimiento preciso sobre algo o para inferir las consecuencias válidas de un hecho". Esta etimología destaca la importancia del dato como un elemento esencial en la obtención de información exacta y en la formulación de conclusiones válidas a partir de hechos (Real Academia Española, 2019).

A partir de lo expuesto, es fundamental destacar las garantías que surgen del reconocimiento de los derechos de carácter personal, los cuales han sido elevados a la categoría de derechos fundamentales. Este reconocimiento protege la capacidad del ser humano para evitar la intromisión no autorizada de funcionarios públicos u otros individuos en aspectos íntimos y privados de su vida (Jalkh Röbens, 2008).

Los derechos personales abarcan una amplia gama de áreas, incluyendo la correspondencia, los pensamientos, el hogar y las comunicaciones. Esto significa que cada persona tiene el derecho a mantener su privacidad y a decidir quién puede acceder a su información personal. Además, este marco legal se extiende a la protección del tiempo libre del individuo, asegurando que las actividades personales no sean objeto de vigilancia o interferencia indebida (Téllez Aguilera, 2001).

Es así como, la interconexión de datos es crucial para dotar de significado a la información, ya que permite que los elementos aislados se transformen en conocimientos valiosos y comprensibles. Esta evolución del concepto de "dato" no solo refleja su origen etimológico, sino que también subraya la importancia de las conexiones y relaciones entre los datos para formar un conjunto coherente de información útil y relevante en diversos contextos (Villalba, 2021).

En este sentido, la categorización de los datos como personales cobra especial relevancia, ya que facilita la creación de perfiles y la deducción de inferencias específicas atribuibles a cada consumidor. Esta capacidad de diferenciación es esencial en un entorno empresarial donde la personalización y el entendimiento profundo de los clientes son fundamentales para lograr un éxito competitivo en mercados específicos (Puccinelli, 1999).

La protección de estos derechos es esencial para garantizar la dignidad y la libertad individual en una sociedad democrática. Al salvaguardar la privacidad y la intimidad, se fomenta un entorno donde las personas pueden expresarse libremente, sin temor a represalias o invasiones en su vida privada. Así, el reconocimiento y respeto por estos derechos fundamentales no solo son un pilar de la justicia social, sino también una condición necesaria para el desarrollo pleno del ser humano en todos los aspectos de su vida (Hernández-Delgado, 2006).

En resumen, el derecho a la protección de datos personales abarca un conjunto integral de derechos, principios y garantías previamente establecidos. Su objetivo principal es prevenir, proteger y reparar los posibles daños que puedan sufrir las personas debido al uso indebido de su información. Así, se busca no solo resguardar la privacidad de los individuos, sino también establecer un marco legal que garantice una gestión ética y responsable de los datos en un contexto donde su valor económico y jurídico es ampliamente reconocido. Esta protección es esencial para fomentar la confianza en las relaciones entre consumidores y empresas, asegurando que la información personal sea tratada con el respeto y la diligencia que merece (Villalba, 2021).

1.2. DERECHO A LA PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

El correcto análisis jurídico para identificar la violación del derecho a la intimidad, tanto en el ámbito público como en el privado, se centra en la falta de un consentimiento válido para acceder a la información personal o para su uso específico. Este enfoque implica evaluar cómo se obtuvo la información y si fue entregada de manera legítima, es decir, con la debida autorización. En este contexto, es crucial determinar si dicha información fue utilizada para propósitos diferentes a los inicialmente consentidos o si, por el contrario, no existió ninguna autorización que justificara su acceso (Villalba, 2021).

La relación entre el consentimiento y la intimidad es fundamental, ya que la ausencia de autorización puede dar lugar a una posible violación del derecho a la privacidad. Este derecho no solo protege la esfera personal de los individuos, sino que también establece límites claros sobre cómo se puede manejar su información. Por lo tanto, al examinar casos de posible invasión a la intimidad, es esencial considerar si el consentimiento fue informado, libre y específico (Gozaíni, 2001).

Además, el marco legal actual, como lo establece la Ley Orgánica de Protección de Datos Personales en Ecuador, refuerza estos principios al garantizar que los ciudadanos tengan control sobre su información personal. La ley estipula que cualquier recolección o tratamiento de datos requiere el consentimiento del titular, lo que significa que las entidades deben actuar con transparencia y respeto hacia los derechos individuales.

Este enfoque no solo busca proteger a los individuos de posibles abusos por parte de terceros, sino que también promueve un entorno donde se respete la dignidad humana y se fomente la confianza en las interacciones personales y comerciales. La protección de datos personales se convierte así en un pilar esencial para garantizar que las personas puedan disfrutar de su derecho a la privacidad sin temor a intromisiones indebidas o al uso inapropiado de su información. En última instancia, este marco legal busca equilibrar las necesidades de las empresas y organizaciones con los derechos

fundamentales de los ciudadanos, asegurando un manejo ético y responsable de los datos personales en todos los ámbitos (Gozaíni, 2001).

Considerando el numeral 11 del artículo 66 de la (Constitución del Ecuador, 2008), que protege de manera general los derechos más fundamentales del ser humano, así como el uso de la información personal que debe estar vinculada a la autorización del titular, se establece una conexión con el numeral 19 de la misma norma. Este último se refiere a lo que hemos definido anteriormente como transferencia de datos, garantizando así la interacción personal de la siguiente manera:

> *El derecho a la protección de datos personales incluye tanto el acceso a la información como la capacidad de decidir sobre su uso y la correspondiente salvaguarda. La recolección, almacenamiento, procesamiento, distribución y difusión de estos datos requieren siempre la autorización del titular o un mandato legal.*

Esta normativa establece que la autorización para el uso de datos es un elemento esencial, basado en el acuerdo tácito entre las partes para generar un efecto específico. Por lo tanto, si el efecto producido es diferente al acordado, es necesario determinar los límites y consecuencias de esa autorización específica. Esto implica evaluar si ha habido un exceso en el uso de los datos otorgados, tanto en el ámbito privado entre individuos como en el sector público (Ordoñez Pineda, 2019).

En este sentido, es fundamental que el consentimiento sea expreso o tácito, pero siempre claro e inequívoco. Si se logra verificar el consentimiento del titular, este se convierte en una causa justificativa para el uso de sus datos. Así, se asegura que cualquier tratamiento de información personal se realice dentro de los parámetros legales establecidos y con el respeto debido a los derechos individuales (Uicich, 1999).

Por otra parte, se encuentran los datos públicos, es decir, información personal que, por su naturaleza y en su totalidad, constituye datos de acceso público. En términos generales, la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) establece que, en principio, se considera información pública todo aquel dato que emane o esté en posesión del Estado, ya sea directamente o a través de

entidades privadas que tengan participación estatal (Registro Oficial No. 337, 2004). Específicamente, la gestión y control de los datos públicos en Ecuador recae en el Estado a través del Sistema Nacional del Registro de Datos Públicos, que incluye organismos como la Dirección Nacional de Registro de Datos Públicos (DINARDAP), la Dirección General de Registro Civil, Identificación y Cedulación, o el Registro de la Propiedad, entre otros. En algunos casos, también se considera que aquellas instituciones privadas que poseen información que, por su naturaleza, es de acceso público, se integran a este sistema y están sujetas a su regulación. Es crucial aclarar que, según lo mencionado, las entidades privadas tienen la facultad de gestionar tanto datos personales de acceso público como privado (Ley Orgánica de Telecomunicaciones, 2015).

1.3. LOS DATOS PERSONALES EN LA GESTIÓN DE COBRANZA

En el contexto específico del uso de datos personales en la gestión de cobranza, es esencial que las empresas respeten estos principios y obligaciones. La gestión adecuada no solo protege los derechos individuales, sino que también fortalece la confianza del consumidor en las prácticas comerciales.

La Ley Orgánica de Protección de Datos Personales (LOPDP) es un marco legal crucial en Ecuador, aprobado el 10 de mayo de 2021, que regula el tratamiento de la información personal de los ciudadanos. Su principal objetivo es garantizar el derecho a la protección de los datos personales, un aspecto esencial en un mundo donde la información se ha convertido en un recurso valioso y vulnerable.

En el contexto de la cobranza extrajudicial en Ecuador en la actualidad, el uso de datos personales se encuentra regulado por varias normativas, garantizando la protección de la privacidad de los ciudadanos. A continuación, se presentan los tipos de uso permitido de los datos personales en este ámbito, en consonancia con la legislación vigente:

1. Identificación de Deudores: Los datos personales pueden ser utilizados para identificar adecuadamente a los deudores, incluyendo su nombre completo, documento de identidad y dirección, siempre con el consentimiento explícito del titular de los datos, conforme lo establece la Ley Orgánica de Protección de Datos Personales (LOPD).

2. Verificación de Información: Las entidades cobranza están facultadas para utilizar datos personales para verificar la información relacionada con la deuda, asegurando la exactitud de los datos antes de iniciar cualquier procedimiento de cobranza. Este uso debe ser proporcional y justificado, alineándose con los principios de necesidad y minimización establecidos por la LOPD.

3. Notificaciones y Comunicaciones: Se permite el uso de datos personales para enviar notificaciones sobre el estado de la deuda, recordatorios de pago y aclaraciones sobre la obligación del deudor. Estas comunicaciones deben ser claras, no engañosas y respetar el derecho del titular a la intimidad.

4. Propuestas de Acuerdo de Pago: La información personal puede ser utilizada para proponer acuerdos de pago, facilitando alternativas que permitan al deudor cumplir con sus obligaciones, en cumplimiento de lo estipulado por la normativa sobre acuerdos de reestructuración de deuda.

5. Registro de Pagos y Cumplimiento: Los datos deben ser utilizados para llevar un registro de los pagos realizados por el deudor y para verificar el cumplimiento de los acuerdos establecidos, asegurando un manejo transparente de la información.

6. Informes a Centrales de Riesgo: En caso de incumplimiento, los datos personales pueden ser reportados a entidades de información crediticia, siempre que se realice conforme a los procedimientos establecidos en la normativa y garantizando que el deudor haya sido informado sobre esta posibilidad.

7. Prevención del Fraude: El análisis de datos personales puede ser llevado a cabo para detectar patrones de comportamiento sospechosos que indiquen posibles fraudes, en línea con la normativa que protege a los acreedores y a otros consumidores.

8. Cumplimiento Normativo y Auditorías: El uso de datos personales en la cobranza extrajudicial deberá cumplir con todas las normativas vigentes, incluyendo el Código Orgánico Integral Penal (COIP), que establece sanciones para el tratamiento ilegítimo de la información. Además, las entidades deben estar sujetas a auditorías que garantizan que sus prácticas se alineen con la LOPD y otras regulaciones pertinentes.

En resumen, el uso de datos personales en la cobranza extrajudicial en Ecuador debe ser realizado de manera responsable y ética, protegiendo siempre los derechos

fundamentales de los deudores y cumpliendo con el marco legal establecido por la legislación ecuatoriana y las normas internacionales aplicables. Las entidades de cobranza deben asegurar que sus procedimientos estén diseñados para respetar la privacidad y la seguridad de la información personal de los ciudadanos.

En 2014, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros implementó un conjunto de normativas conocidas como las Disposiciones de Carácter General para las Entidades Financieras en relación con los Despachos de Cobranza. Estas regulaciones fueron diseñadas con el propósito de establecer un marco claro que regule las prácticas de cobranza realizadas por los despachos encargados de gestionar las carteras de crédito de las instituciones financieras.

Es fundamental que los despachos eviten prácticas abusivas o engañosas. Por ejemplo, no pueden utilizar nombres o términos que se asemejen a instituciones públicas, ni amenazar o intimidar a los deudores o a sus familiares. Asimismo, está prohibido realizar gestiones de cobro a personas ajenas a la deuda, salvo en el caso de co-deudores o avales. También se prohíbe el envío de documentos que puedan parecer escritos judiciales o que intenten hacerse pasar por representantes de alguna autoridad judicial (Villalba, 2021).

La implementación rigurosa de estas normativas es esencial no solo para proteger los derechos de los usuarios de servicios financieros, sino también para prevenir sanciones que podrían derivarse del incumplimiento. El respeto por estas reglas contribuye a fomentar un entorno más justo y transparente en el ámbito financiero, promoviendo prácticas responsables en la gestión de cobranzas. Así, se busca equilibrar la necesidad de recuperar créditos con la obligación ética de tratar a los consumidores con dignidad y respeto, asegurando que sus derechos sean salvaguardados en todo momento (Ordoñez Pineda, 2019).

Además, es importante destacar que el incumplimiento de las normativas sobre protección de datos puede resultar en daños colaterales para los consumidores. El mal uso de su información personal puede llevar a situaciones como el acoso por parte de cobradores, la suplantación de identidad o incluso la exclusión de servicios financieros esenciales. Estos efectos no solo afectan la situación económica del individuo, sino que

también pueden tener repercusiones en su salud mental y bienestar general (Hernández-Delgado, 2006).

La ley exige que las empresas obtengan un consentimiento libre e informado antes de utilizar los datos personales, lo que implica que los usuarios deben ser plenamente conscientes del tipo de información que están compartiendo y del propósito específico para el cual se utilizará. En caso de que una entidad financiera o un despacho de cobranza actúe sin este consentimiento o utilice los datos para fines no autorizados, se considera una violación grave del derecho a la privacidad (Hernández-Delgado, 2006).

Por otro lado, la doctrina sostiene que la garantía jurisdiccional del habeas data protege el derecho a la protección de datos personales, ya que esta figura legal resguarda cualquier dato personal que esté bajo la custodia o administración del Estado o de entidades privadas. Naranjo (2017) argumenta que esta garantía facilita el ejercicio de los derechos ARCO, que se refieren al acceso, rectificación, cancelación y oposición de los datos personales. Sin embargo, es importante hacer algunas aclaraciones sobre la disposición constitucional para definir claramente qué objeto se encuentra tutelado.

CAPÍTULO II

2.1. USO DE DATOS PERSONALES Y AFECTACIÓN AL DERECHO A LA PRIVACIDAD

En respuesta a la variedad de peligros y amenazas en el ámbito digital, Ecuador, antes de la implementación de la Ley Orgánica de Protección de Datos Personales, definió un método para hacer efectivos los derechos de consulta y corrección, que todas las entidades gubernamentales a cargo del manejo de información personal debían poner en práctica (Acuerdo Ministerial 012-2019, 2019). Este método se integró a la política de cada institución sobre la protección de datos personales, buscando asegurar el completo ejercicio de estos derechos. Hoy en día, con la aplicación de la ley mencionada, el dueño de los datos no solo puede acceder a los derechos ya mencionados, sino que también puede ejercer los derechos a la supresión, al rechazo y a la transferencia de sus datos, frente a quienes los manejan, ya sean entidades públicas o empresas privadas, nacionales o extranjeras.

Por lo tanto, quienes manejan o son responsables del manejo de datos deben crear los medios para que estos derechos se puedan ejercer en su totalidad, respetando los siguientes principios legales: a) acceso: el dueño de los datos puede pedir información detallada de sus datos personales y debe ser respondido en un plazo de 15 días; b) corrección y actualización: el dueño de los datos puede pedir que se corrijan o actualicen datos personales que sean incorrectos o estén incompletos, y se le responderá en 15 días; c) supresión u olvido: el dueño de los datos puede pedir que se borren sus datos personales si el manejo de estos no ha cumplido con las leyes correspondientes; esta petición se responderá en 15 días; d) rechazo: el dueño de los datos puede oponerse a que sus datos personales se usen para fines de publicidad o que afecten sus derechos básicos; esta petición se responderá en 15 días; y, e) transferencia, sobre lo cual la Autoridad de Protección de Datos Personales dará a conocer el método específico.

Considerando todo lo mencionado, es crucial establecer los criterios de protección y justificar su estructura, ya que su cumplimiento asegura el pleno ejercicio del derecho a la autodeterminación. Un criterio es un conjunto de requisitos que sirven como herramienta para el manejo de datos personales. En el ámbito de la protección de datos, estos son requisitos básicos pero esenciales. Ignorar alguno de estos violaría el derecho fundamental a la protección de datos personales.

El consentimiento, como manifestación de la voluntad, es la forma ideal de expresarla. En el contexto del derecho a la protección de datos personales, se refiere a la aceptación o rechazo del titular al manejo de sus datos personales. Diversos autores como Garriga, Rebollo y Serrano, y Troncoso, afirman que el consentimiento debe cumplir con ciertas características, respondiendo al estándar de ser libre, específico, inequívoco e informado.

- Primer requisito: consentimiento libre. El titular de los datos debe dar su consentimiento de forma voluntaria, sin coacción.
- Segundo requisito: consentimiento específico. La aceptación del manejo de datos debe estar dirigida a un propósito concreto.
- Tercer requisito: consentimiento informado. El titular debe ser consciente y entender los hechos y las implicaciones que se derivan de su prestación, lo que relaciona directamente con la noción de control y autodeterminación.
- Cuarto requisito: consentimiento inequívoco. No debe haber duda sobre la voluntad del titular de aceptar el manejo de sus datos personales.

Además del consentimiento del titular, la legitimidad del manejo de datos personales puede ser otorgada por mandato legal, ejecución de un contrato y orden de autoridad competente. A pesar de las distintas formas de legitimar el manejo de datos personales, el consentimiento es la regla general y un pilar fundamental.

Partiendo de que existen distintas maneras para que el manejo sea legítimo, estas deben estar dirigidas a un propósito. Aquí radica la importancia del principio de finalidad, que se manifiesta como una garantía fundamental mediante la cual se presenta a los titulares de los datos personales la posibilidad de controlar el manejo de estos. Los datos personales deben ser recogidos con fines determinados y explícitos y no serán tratados posteriormente con fines contrarios para los que fueron recogidos.

Una razón justificada para usar datos personales debe apegarse a las reglas legales. Aunque el uso de los datos coincida con la razón original, no es válido si va en contra de la ley. Además, la razón debe ser clara y específica, evitando propósitos amplios, confusos o indefinidos.

En Ecuador, la ley protege al consumidor de prácticas de cobranza abusivas. Los proveedores y las empresas de cobranza que actúen en su nombre deben abstenerse de

exponer al deudor al ridículo, la difamación, la coacción ilícita o cualquier tipo de amenaza. El cumplimiento de esta obligación no impide que se tomen acciones penales si corresponde.

Las empresas de cobranza que gestionan el cobro por teléfono, mensajes o correo electrónico están sujetas a restricciones específicas:

- Solo se permite una comunicación diaria por el mismo medio.
- Las comunicaciones deben realizarse entre las 7:00 y las 20:00, de lunes a viernes1. Se prohíben los fines de semana y feriados.
- Las llamadas deben realizarse desde números identificables.
- Está prohibido hostigar, intimidar o molestar al deudor de manera insistente.

Se consideran acciones de hostigamiento:

- Realizar comunicaciones de cobro que no cumplan con las restricciones horarias y de frecuencia mencionadas.
- Comunicarse con personas que no sean el deudor, codeudor o garante para tratar el tema de la deuda.

Si se vulneran estos derechos, el consumidor puede presentar una denuncia ante el Defensor del Cliente de la institución financiera, la Superintendencia de Bancos, la Superintendencia de Compañías o la Defensoría del Pueblo1. Las entidades que incumplan estas disposiciones pueden ser sancionadas con multas de hasta $4.500 dólares, y en caso de reincidencia, el doble

2.2. EFECTOS JURÍDICOS DEL USO INDEBIDO DE DATOS PERSONALES

El 26 de mayo de 2021, Ecuador marcó un hito en la protección de la privacidad con la publicación de la Ley Orgánica de Protección de Datos Personales (en adelante, "la Ley") en el Registro Oficial Suplemento 459. Esta legislación pionera tiene como objetivo central asegurar que todos puedan ejercer su derecho fundamental a la protección de sus datos personales, incluyendo el control sobre su información y la garantía de su seguridad (Artículo 1). Para lograrlo, la Ley establece principios, derechos, deberes y mecanismos de protección que deben ser respetados por todas las entidades, tanto

públicas como privadas. Además, la Ley tiene alcance en todo el territorio ecuatoriano, protegiendo los datos de los ciudadanos incluso si son procesados fuera del país.

Con el propósito de garantizar el ejercicio del derecho fundamental a la protección de datos personales, la ley también tiene alcance extraterritorial, asegurando la protección de los datos personales de los ciudadanos ecuatorianos incluso cuando estos sean procesados fuera del país. Además, reconoce que el tratamiento de datos personales requiere el consentimiento válido del titular, el cual debe ser otorgado de manera libre, específica, informada e inequívoca. Esto significa que las personas tienen la capacidad de decidir sobre el uso de su información con base en un conocimiento claro sobre quién la procesa, cómo se utiliza, cuándo y con qué finalidad.

La Ley también enfatiza que el consentimiento para el uso de datos personales debe ser otorgado libremente, de manera específica, con pleno conocimiento y sin lugar a dudas. Esto significa que cada persona tiene el derecho de decidir, basándose en una comprensión clara, quién usará su información personal, cómo, cuándo y con qué propósito. La normativa también exige que el tratamiento de datos personales tenga un fin legítimo, el cual puede ser supervisado por la Autoridad de Protección de Datos Personales. Con estas bases establecidas, es importante definir legalmente qué se considera un "dato personal".

El artículo 4 de la Ley establece que un dato personal es cualquier información que pueda identificar, directa o indirectamente, a una persona. Esto significa que la información protegida puede ser de cualquier tipo y estar en cualquier formato, siempre y cuando permita identificar a una persona, ya sea con o sin la ayuda de sistemas informáticos. Por lo tanto, expertos como Gil (2015) argumentan que la lista de datos personales debe ser amplia y adaptable, incluyendo no solo información sobre identidad, finanzas, trabajo o religión, sino también el comportamiento digital de una persona, es decir, su "huella digital". En resumen, la Ley regula el uso de una amplia gama de datos personales, y un manejo inadecuado de esta información podría afectar el ejercicio de otros derechos fundamentales.

La Ley establece 16 principios fundamentales que guían el sistema de protección de datos personales, basándose en normas internacionales y en la doctrina. Principios como la lealtad, transparencia, finalidad, minimización, proporcionalidad,

confidencialidad, exactitud y conservación fueron reconocidos inicialmente en las Directrices de la OCDE (1980), la Resolución 45/95 de la ONU (1990) y la Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas (2012). Además, la "responsabilidad proactiva" se ha analizado desde perspectivas innovadoras como "Privacidad desde el Diseño" y "Resiliencia Cibernética", que exigen a quienes manejan datos personales un mayor nivel de responsabilidad.

La Ley también reconoce una serie de derechos para garantizar la protección efectiva de los datos personales. Entre ellos, el derecho a la información es crucial, ya que asegura que cada persona sea informada de manera clara y honesta sobre los fines del tratamiento de sus datos, la base legal, el tiempo de conservación, la identidad del responsable y las posibles consecuencias.

Entre otras contribuciones importantes, la Ley identifica cuatro categorías especiales de datos personales cuyo tratamiento está prohibido o limitado. Estas categorías incluyen datos sensibles, datos de niños y adolescentes, datos de salud y datos de personas con discapacidad (y de sus representantes, en relación con la discapacidad). Dentro de la categoría de datos sensibles, la Ley distingue: 1) datos de personas fallecidas, que pueden ser solicitados, corregidos, actualizados o eliminados por sus herederos, a menos que la persona fallecida haya especificado lo contrario en vida; y 2) datos crediticios, que solo pueden ser utilizados para evaluar negocios, el historial comercial o la capacidad de pago de una persona.

Se enfatiza que, a pesar de la situación actual, los ciudadanos tienen la posibilidad de presentar denuncias ante entidades de control, como la Fiscalía, para frenar el uso indiscriminado de su información por parte de las empresas.

Una recomendación práctica es que, al recibir una llamada de cobranza, el consumidor debe preguntar quién proporcionó su información y anotar el número de teléfono para formalizar la denuncia. Esta acción no solo pone de manifiesto el empoderamiento del individuo en la protección de su información personal, sino que también establece un precedente de que no se tolerará el uso abusivo de los datos.

La sensibilidad de los datos personales se determina en función del daño que podría causar a una persona la divulgación pública de dicha información. En otras palabras, las categorías especiales de datos personales son aquellas cuyo tratamiento

indebido podría afectar directamente la privacidad de una persona y el ejercicio de otros derechos fundamentales (Pérez, 2015). Ejemplos de esta categoría, que requiere un tratamiento legal especial, son las finanzas, la salud o el origen étnico (Gil, 2015).

Por otro lado, la Ley permite la transferencia o comunicación de datos personales a terceros siempre que existan propósitos legítimos, que estén relacionados con las funciones del responsable del tratamiento o del destinatario y que se cuente con el consentimiento del titular. De esta manera, la Ley restringe la transferencia de información personal para proteger a los ciudadanos de usos malintencionados que puedan afectar su integridad o sus derechos. Sin embargo, la norma también establece que no se considerará transferencia de datos cuando exista un contrato que defina claramente los fines y límites del procesamiento de los datos personales.

En cuanto a la seguridad de los datos personales, la Ley exige que quienes manejan datos implementen diversas medidas para evitar posibles violaciones de derechos. Estas medidas incluyen la anonimización, la seudonimización y la protección desde el diseño y por defecto, las cuales han sido ampliamente reconocidas en instrumentos internacionales como el Reglamento Europeo de Protección de Datos (2016). Sobre estos mecanismos, Martínez-Martínez (2018) destaca la importancia de que quienes procesan información personal asuman la responsabilidad desde su propia realidad, respetando siempre la libertad de decisión del titular y su derecho a ser informado previamente. En definitiva, la protección efectiva requiere acciones conjuntas del Estado, los titulares y los responsables del tratamiento de datos.

La Ley también establece 15 obligaciones que deben cumplir quienes manejan datos personales, incluyendo el uso de procesos y herramientas legítimas, la implementación de sistemas de evaluación y verificación de la seguridad, el desarrollo de políticas de prevención de riesgos y la oferta de mecanismos de protección. De esta manera, la Ley busca definir claramente las responsabilidades de este actor fundamental, que tiene el acceso y control de los datos personales. En la misma línea, se prevé la designación de un delegado de protección de datos personales cuando el tratamiento sea realizado por un actor público, sea a gran escala y verse sobre categorías especiales de datos, o esté relacionado con la seguridad y defensa nacional. El delegado tendrá funciones de asesoría, supervisión y cooperación, actuando como un aliado importante de la Autoridad de Protección de Datos Personales.

En concordancia con los instrumentos internacionales, la Ley permite la transferencia internacional de datos personales a países, organizaciones o personas jurídicas que ofrezcan niveles adecuados de protección y se sujeten a los estándares internacionales. Para ello, se establece un régimen específico de mecanismos de control, que incluye el reconocimiento por parte de la Autoridad de Protección de Datos de que el receptor cuenta con un sistema de protección adecuado y la provisión de garantías suficientes por parte del encargado del tratamiento. En este sentido, la Ley reconoce la importancia de los flujos internacionales de información personal, que en la era digital son fundamentales para establecer relaciones de comercio y cooperación.

2.3. MEDIDAS DE PREVENCIÓN DEL USO DE DATOS PERSONALES

En cuanto al régimen disciplinario, la Ley establece medidas correctivas que se aplicarán cuando no se hayan cumplido las disposiciones legales en materia de protección de datos personales. Estas medidas incluyen el cese del procedimiento, la eliminación de datos y la imposición de medidas técnicas, jurídicas o administrativas. Además, la Ley prevé sanciones económicas que serán aplicadas por la Autoridad de Protección de Datos Personales, respetando el principio de proporcionalidad. Las sanciones leves implican el pago de uno a diez salarios básicos unificados o una multa de 0.1% a 0.7% del volumen del negocio de la organización privada, mientras que las sanciones graves implican el pago de diez a veinte salarios básicos unificados o una multa de 0.7% a 1% del volumen del negocio de la organización privada.

En el ámbito de la institucionalidad, la Ley dispone la creación de la Autoridad de Protección de Datos Personales, que será responsable de garantizar el derecho a la protección de datos personales y de controlar el cumplimiento de la ley, su reglamento y las regulaciones que dicte. Para lograr sus objetivos, la Ley otorga a este órgano funciones de regulación, control, legislación y ejecución, todas ellas encaminadas a proteger los derechos y libertades fundamentales de las personas en relación con el tratamiento de sus datos personales.

El marco legal de Ecuador históricamente ha carecido de regulaciones integrales en áreas críticas, lo que dificulta la plena realización de los derechos constitucionales. Los derechos de protección de datos, en particular, han experimentado un progreso limitado. El habeas data sirve como un mecanismo para proteger la privacidad individual en medio de la creciente digitalización. La Corte Constitucional ha definido el habeas

data como una acción constitucional para salvaguardar el derecho a la privacidad, reconociendo que no toda la información personal es pública y libremente divulgable.

La Constitución de la República del Ecuador (CRE) de 2008 y la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (Ley de Garantías) establecen el habeas data como el recurso legal para que los individuos accedan a la justicia constitucional con respecto a sus datos personales. Esto permite a las personas apelar a un juez si su solicitud para acceder, supervisar, actualizar, rectificar, eliminar o anular cualquier registro que contenga sus datos no es atendida. La Corte Constitucional describe esta acción como un mecanismo rápido para que las personas conozcan sus datos y su propósito, ya sea en bases de datos públicas o privadas, enfatizando su papel en garantizar el acceso y control sobre la información personal y proteger la privacidad y la autodeterminación informativa.

A pesar de ser un paso hacia la garantía de los derechos constitucionales, los derechos de privacidad aún carecen de salvaguardias adecuadas. La ausencia de un plazo específico para presentar una acción de habeas data crea vulnerabilidad, ya que el artículo 50 de la Ley de Garantías solo menciona su disponibilidad en caso de denegación o violación de derechos, sin especificar un plazo razonable después de una denegación.

Persisten preguntas significativas sobre las mejores prácticas para la difusión y el manejo de datos en Ecuador. El marco legal carece de claridad sobre la permisibilidad de acciones legales contra el manejo inadecuado de datos, la configuración del consentimiento para la divulgación de datos personales y otros temas relacionados. Los artículos existentes sugieren que las personas en Ecuador pueden emprender acciones legales para corregir aspectos no regulados, sin embargo, esta laguna regulatoria permite a las entidades privadas manejar la información del consumidor con considerable discreción. Abordar esta laguna es crucial para fortalecer los derechos individuales de privacidad y la gestión de datos personales en Ecuador.

En la era digital, los datos personales son tanto un activo comercial como un objetivo para nuevas formas de delincuencia. La limitada protección de los datos personales en Ecuador exige un análisis desde la perspectiva del derecho penal, donde el interés jurídico protegido varía según el delito específico. Según Jijena Leiva, proteger los datos personales implica su correcta recopilación, administración, actualización continua, uso específico y derechos de acceso irrestrictos. Los delitos informáticos, como

categoría, abarcan acciones indebidas que dañan el interés jurídico protegido, perjudicando la integridad de los equipos y la privacidad de sus propietarios.

El Código Orgánico Integral Penal (COIP) de Ecuador buscó modernizar el sistema legal introduciendo nuevas clasificaciones sin evaluar completamente su eficacia práctica. Por ejemplo, el artículo 178 del COIP tipifica como delito la violación de la intimidad, penalizando teóricamente la difusión, el acceso o la divulgación no autorizados de información privada a través de cualquier medio. Esta disposición penaliza ampliamente las acciones ilegales que afectan la privacidad e incluye una sección para sancionar las conductas que amenazan la confidencialidad, la integridad y la disponibilidad de los datos, considerando los sistemas informáticos como un activo jurídico protegido.

Sin embargo, la legislación carece de una guía clara sobre qué comportamientos de procesamiento de datos son poco éticos o no autorizados, a pesar de su prevalencia en las prácticas comerciales estándar. Aunque existen algunas sanciones, como las del Código Orgánico Monetario y Financiero que prohíben la venta de bases de datos de clientes, sigue existiendo una amplia gama de delitos que afectan la privacidad personal a través de los datos personales. Esta ambigüedad regulatoria permite a las empresas una considerable discreción en el manejo de la información de los consumidores, lo que subraya la necesidad de abordar estas lagunas legales para mejorar la protección de los derechos individuales en materia de privacidad y gestión de datos personales en Ecuador.

La promulgación de la Ley Orgánica de Protección de Datos Personales en mayo de 2021 representa un importante paso adelante, que refleja las influencias de la normativa europea y hace hincapié en la protección de los derechos personales. Esta ley tiene como objetivo garantizar los derechos de los ciudadanos a controlar su información personal, estableciendo principios, derechos, obligaciones y mecanismos de protección.

CONCLUSIÓN

- La evolución continua de las Tecnologías de la Información y la Comunicación (TIC) plantea retos constantes, a menudo haciendo que los mecanismos legales existentes para la protección de datos personales resulten insuficientes. La sociedad demanda cada vez más enfoques transparentes, lícitos y modernos para salvaguardar los derechos fundamentales, junto con estrategias innovadoras para comprender la magnitud de las ciberamenazas. Esto requiere un cambio desde medidas reactivas hacia soluciones integrales y proactivas que aborden de manera efectiva el panorama dinámico de la seguridad digital.
- Si bien se han intentado iniciativas legislativas para proteger los datos personales en Ecuador, ninguna ha logrado plasmarse en un marco regulatorio sólido y definitorio. La problemática, aunque abordada en el contexto de la relación empresa-cliente, trasciende este ámbito específico. La ausencia de mecanismos efectivos para salvaguardar la información del consumidor no es solo una deficiencia en este vínculo, sino una carencia generalizada. Esta falta de un sistema integral de protección de datos personales convierte a cada individuo en un sujeto vulnerable, subrayando la imperiosa necesidad de un avance legislativo urgente que colme este vacío legal en el país.
- A pesar de los esfuerzos legislativos incompletos para proteger los datos personales en Ecuador, persiste una vulnerabilidad generalizada. La autodeterminación informativa, que faculta a los individuos a controlar su información personal y decidir su estatus público o privado, se ve comprometida por la falta de regulaciones claras. La vulneración de la privacidad ocurre cuando la información se transfiere sin un consentimiento expreso o tácito válido, cediendo el control de los datos a terceros. Esta situación subraya la urgente necesidad de un marco legal sólido que garantice la protección de los datos y respete la autodeterminación informativa de cada individuo en Ecuador.

RECOMENDACIONES

- Es imperativo concretar la aprobación de leyes que establezcan regulaciones efectivas para la protección de datos personales, subsanando las deficiencias evidenciadas y adaptándose a las necesidades actuales. Además, se requiere el desarrollo de mecanismos de protección del consumidor más sólidos y accesibles, que ofrezcan un amparo real y tangible frente a las potenciales vulneraciones a la privacidad.
- Impulsar activamente la creación de una cultura de privacidad a través de campañas de sensibilización y programas educativos dirigidos tanto a consumidores como a empresas. El objetivo es fomentar una conciencia más profunda sobre el valor de la protección de datos y las responsabilidades inherentes, contribuyendo así a una sociedad donde la privacidad sea un pilar fundamental.
- Antes de utilizar cualquier dato personal para actividades de cobranza, es crucial obtener el consentimiento claro e informado del titular de los datos. Esto implica que los deudores deben ser informados sobre qué datos se recopilan, con qué propósito se utilizarán, y quién tendrá acceso a esa información. Este cumplimiento con los principios de transparencia y legitimidad no solo es un requisito legal, sino que también garantiza el respeto hacia los derechos de los individuos y ayuda a construir una relación más ética y responsable con los clientes

REFERENCIAS BIBLIOGRÁFICAS

Anchundia, A. (2022). En síntesis, la doctrina establece que la Libertad Personal es un derecho fundamental que puede perderse como consecuencia de actos que perjudican a terceros, como agresiones físicas o verbales, así como por la comisión de delitos tipificados por la ley. . *INREDH*, 10.

Barocelli, S. (2020). Prácticas abusivas en el cobro extrajudicial de deudas a presuntos deudores en las relaciones de consumo. *Revista Jurídica del Colegio de Abogados Zárate Campana*, 10.

Benavides Ordoñez, J., & Escudero Soliz, J. (2013). *Manual de justicia constitucional ecuatoriana.* Quito: Corte Constitucional, Cuadernos de Trabajo No. 4.

Constitución de la República del Ecuador. (2008). QUITO: Corporación de Estudios y Publicaciones.

Constitución del Ecuador. (2008). *Constitución del Ecuador.* Quito: CEP.

Corte Constitucional del Ecuador, 98-23-JH y acumulados (13 de Diciembre de 2023).

Derecho a la salud de personas privadas de la libertad, No. 209-15-JH y 359-18-JH acumulados (Corte Constitucional 12 de Noviembre de 2019).

Gozaíni, O. A. (2001). *Hábeas data. Protección de datos personales: doctrina y jurisprudencia.* Buenos Aires: Editorial Rubinzal.

Habeas corpus, Sentencia: No. 365-18-JH/21 (Corte Constitucional 2021).

Hernández-Delgado, V. (2006). Referentes legales para un marco protector de datos personales. *Revista Rs Ximhai*, 10-18.

Jalkh Röbens, G. (2008). *Neoconstitucionalismo y sociedad. Serie Justicia y Derechos Humanos* . Quito: Justicia y Derechos Humanos.

López, J. F. (15 de julio de 2007). *Foro de consultas archivo*. Obtenido de Hispanoteca Lengua y Cultura: https://web.archive.org/web/20070615173126/http://culturitalia.uibk.ac.at/hispanoteca/Foro-preguntas/ARCHIVO-Foro/H%C3%A1beas%20corpus.htm

Ordoñez Pineda, L. (2019). El procedimiento de solicitud de adecuación de los datos de conformidad con la identidad de género. Reflexiones desde el derecho fundamental a la protección de datos . *Foro: Revista de Derecho*, 179-198.

Perdomo, A. P. (1995). *Estudio general sobre el Habeas Corpus.* Medellin: Teoría del colo UCC.

Puccinelli, O. (1999). *El Habeas Data en Indoiberoamérica.* Bogotá: Temis.

Puente, F., & Guerra, M. (2023). La desnaturalización del hábeas correctivo en el Ecuador, análisis del proceso número 24202-2022-00017T. *Revista de Ciencias Sociales y Humanidades*, 12.

Real Academia Española. (2019). *Término Dato.* Madrid: RAE.

Revista Progreso. (20 de febrero de 2021). *Fundación BBVA Microfinanzas*. Obtenido de Progreso: https://www.fundacionmicrofinanzasbbva.org/revistaprogreso/cobranza-extrajudicial-derechos-los-consumidores/

Salgado, H. (2003). *Lecciones de Derecho Constitucional.* Quito: Ediciones Abya-Yala.

Téllez Aguilera, A. (2001). *Nuevas tecnologías. Intimidad y protección de datos.* Madrid: Edisafer.

Uicich, R. (1999). *Los bancos de datos y el derecho a la intimidad.* Buenos Aires: Marcial Pons.

Unidad Judicial Multicompetente, 24202-2022-00017T (Multicompetente 2022).

Vedia, A. D. (1963). *DE VEDIA, AGUSTÍN, Derechos constitucional y administrativo. Instituciones del derecho público,*. Buenos Aires: Macchi.

Villalba, A. (2021). Reflexiones jurídicas sobre la protección de datos y el derecho a la intimidad en la autodeterminación informativa. *Revista Ecuatoriana de Derecho*, 20.

Wilkins, J. (2018). Cobranza extrajudicial Marco regulatorio nacional y ejemplos normativos extranjeros. *Revista de la Biblioteca del Congreso Nacional de Chile*, 15.

DECLARACIÓN Y AUTORIZACIÓN

Nosotros, **Pico Trujillo, Iván Rafael**, con C.C: # **0924111123,** y **Estupiñán Cervantes, José René,** con C.C.: # **0804331254** autores del trabajo de titulación: **EFECTOS DEL USO INDEBIDO DE DATOS PERSONALES EN LA GESTIÓN EXTRAJUDICIAL DE COBRANZA,** previo a la obtención del título de **Abogado** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaramos tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizamos a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, **20** de **febrero** de **2025**

f. _____
PICO TRUJILLO IVÁN RAFAEL

f. _____
ESTUPIÑÁN CERVANTES JOSÉ RENÉ

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	EFECTOS DEL USO INDEBIDO DE DATOS PERSONALES EN LA GESTIÓN EXTRAJUDICIAL DE COBRANZA		
AUTOR(ES)	Iván Rafael Pico Trujillo, José Rene Estupiñán Cervantes		
REVISOR(ES)/TUTOR(ES)	Ab. Marco Antonio Elizalde Jalil		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	**Facultad de Jurisprudencia y Trabajo Social**		
CARRERA:	**Jurisprudencia**		
TITULO OBTENIDO:	**Abogado**		
FECHA DE PUBLICACIÓN:	20 de febrero del 2025	**No. DE PÁGINAS:**	24
ÁREAS TEMÁTICAS:	Derecho Civil, Derecho Constitucional, Derecho Informático		
PALABRAS CLAVES/ KEYWORDS:	Datos personales, Gestión de cobranza, Derecho a la privacidad, Efectos jurídicos, Abuso		

RESUMEN/ABSTRACT:

El uso indebido de datos personales en la gestión extrajudicial de cobranza vulnera el derecho a la privacidad, generando un conflicto entre la recuperación de deudas y la protección de los derechos de los deudores. Las empresas, al implementar tecnologías de análisis de datos para optimizar la cobranza, pueden incurrir en prácticas invasivas, como llamadas frecuentes, mensajes en horarios inoportunos o el rastreo digital, lo cual afecta la privacidad de los individuos. Este escenario plantea dilemas éticos y legales sobre la proporción de las medidas adoptadas, y hasta qué punto el uso de estos datos está justificado sin afectar la intimidad del deudor. En el presente trabajo se pretende abordar como el uso indebido de datos personales vulnera el derecho a la privacidad en la gestión de cobranza de las empresas, ya que se ha vuelto fundamental en el contexto actual, marcado por la digitalización y la expansión de las tecnologías de información. Si bien estas herramientas permiten a las organizaciones mejorar sus procesos de recuperación de deudas, también generan preocupaciones significativas sobre la privacidad de los individuos. Este estudio examina cómo las prácticas de gestión de cobranza impactan el derecho a la intimidad de los deudores, abordando temas como la recopilación y almacenamiento de datos personales, el uso de tecnologías avanzadas para localizar deudores y la comunicación a través de diversos canales que pueden resultar invasivos.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** 0998154116 0939145184	E-mail: ivan.r.pico.t@gmail.com, josereneps42017@gmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre: Reynoso Gaute, Maritza Ginette**	
	Teléfono: +593-4-3804600	
	E-mail: maritza.reynoso@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	