UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS SOCIALES Y SALUD
CARRERA DE DERECHO

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADOS

TÍTULO:
CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023

AUTORES:

LUZ PATRICIA BORBOR SUÁREZ
WILSON JAILMAR CHACA BRAVO

TUTORES:
AB. WASBRUM TINOCO WILFRIDO GIOVANNY, Msc.
ING. SUÁREZ LINDAO BOLIVAR GEOVANNY, Mgt.

LA LIBERTAD – ECUADOR

2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS SOCIALES Y SALUD CARRERA DE DERECHO

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DE TÍTULO DE ABOGADOS

TÍTULO:

CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023

AUTORES:

LUZ PATRICIA BORBOR SUÁREZ

WILSON JAILMAR CHACA BRAVO

TUTORES:

AB. WASBRUM TINOCO WILFRIDO GIOVANNY, Msc

ING. SUÁREZ LINDAO BOLIVAR GEOVANNY, Mgt.

LA LIBERTAD- ECUADOR

2024

La Libertad, 05 de junio de 2024

APROBACIÓN DEL TUTOR

CERTIFICO

Que he analizado el trabajo de integración curricular con el título **"CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023"** presentado por los estudiantes **LUZ PATRICIA BORBOR SUÁREZ y WILSON JAILMAR CHACA BRAVO,** portadores de las cédulas de ciudadanía N.º 0928140920 y N.º 2450032368 respectivamente, como requisito previo a optar el título de **ABOGADOS**, y declaro que luego de haber orientado científica y metodológicamente su desarrollo, el referido proyecto de investigación se encuentra concluido en todas sus partes cumpliendo así con el proceso de acompañamiento determinado en la normativa interna, recomendando se inicien los procesos de evaluación que corresponden.

Atentamente

Ab. Wasbrum Tinoco Wilfrido, Msc
TUTOR

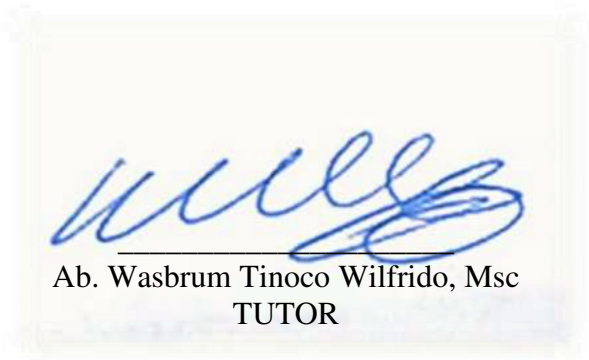
Ing. Suárez Lindao Bolívar, Mgt
TUTOR

La Libertad, 05 de junio de 2024

CERTIFICACIÓN ANTIPLAGIO

En mi calidad de Tutor del Trabajo de Unidad de Integración Curricular: **"CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS EN EL ÁMBITO PRIVADO, 2023 "**, cuya autoría corresponde a los estudiantes **LUZ PATRICIA BORBOR SUÁREZ** y **WILSON JAILMAR CHACA BRAVO** de la carrera de Derecho, CERTIFICO, que el contenido de dicho trabajo ha sido sometido a la validación en sistema anti plagio COMPILATIO, obteniendo un porcentaje de similitud del 5%, cumpliendo así con los parámetros técnicos requeridos para este tipo de trabajos académicos.

Atentamente



Ab. Wasbrum Tinoco Wilfrido, Msc
TUTOR

Lic. Mariela Kathalina Alfonso Villón MSc.
Celular 0998647979
Correo: cutemariel06@gmail.com

La Libertad, 07 de junio de 2024

CERTIFICACIÓN GRAMATICAL Y ORTOGRÁFICA

Yo Mariela Kathalina Alfonso Villón, en mi calidad de LICENCIADA EN CIENCIAS DE LA EDUCACIÓN Y MÁSTER EN ADMINISTRACIÓN DE LA EDUCACIÓN, por medio de la presento tengo a bien indicar que he leído y corregido el trabajo de integración curricular previo a la obtención del título de abogado, denominado "CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023" correspondiente a los estudiantes LUZ PATRICIA BORBOR SUÁREZ Y WILSON JAILMAR CHACA BRAVO de la carrera de derecho de la Universidad Estatal Península de Santa Elena.

Certifico que está redactado con el correcto manejo de lenguaje, claridad en las expresiones, coherencia en los conceptos e interpretaciones. Además de haber sido escrito de acuerdo con las normas de ortografía y sintaxis vigente.

En cuanto puedo decir en honor a la verdad y autorizo a los interesados hacer uso del presente como estime conveniente.

Lic. Mariela Alfonso Villon MSc.
C.I. 0919792408
LICENCIADA EN CIENCIAS DE LA EDUCACIÓN
MAGIST ER EN ADMNISTRACIÓN EDUCATIVA
Registro SENESCYT: 6043188.403

La Libertad, 05 de junio de 2024

DECLARACIÓN DE AUTORÍA

Nosotros Luz Patricia Borbor Suárez y Wilson Jailmar Chaca Bravo, estudiantes del octavo semestre de la carrera de Derecho de la Universidad Estatal Península de Santa Elena, habiendo cursado la asignatura Unidad de Integración Curricular II, declaramos la autoría de la presente propuesta de investigación, de título "Consentimiento en el uso de datos sensibles y la Ley Orgánica de Protección de Datos Personales en el ámbito privado, 2023", desarrollada en todas sus partes por los suscritos estudiantes con apego a los requerimientos de la ciencia del derecho, la metodología de la investigación y las normas que regulan los procesos de titulación de la UPSE.

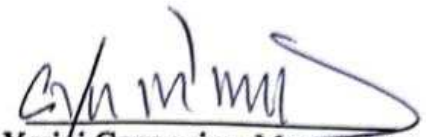
Atentamente

Luz Patricia Borbor Suárez
CC. 0928140920

Wilson Jailmar Chaca Bravo
CC. 2450032368

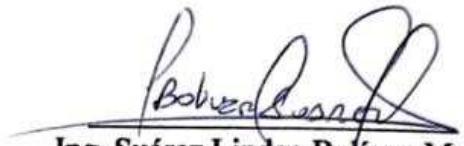
APROBACIÓN DEL TRIBUNAL DE GRADO

Ab. Víctor Coronel Ortiz Mgt.
DIRECTOR DE LA CARRERA



Ab. Yerini Conopoima Moreno, Mgt.
DOCENTE ESPECIALISTA

Ab. Wasbrum Tinoco Wilfrido, Mgt
TUTOR



Ing. Suárez Lindao Bolívar, Mgt
TUTOR

Ab. Brenda Reyes Tomalá, Mgt.
DOCENTE UIC

DEDICATORIA

A mi familia, por ser mi pilar fundamental. A mi mamá, cuya guía, amor incondicional y sacrificio constante me han dado la fortaleza para superar todos los obstáculos. A mis hermanos, tías y a mi abuelita, por su comprensión, aliento y por estar siempre a mi lado en los momentos difíciles y en los de celebración. Cada uno de ustedes ha sido una fuente inagotable de motivación e inspiración.

A mi Pochi, por acompañarme en mis noches en que no dormía, que me ha dado innumerables momentos de felicidad, cuyo amor incondicional ha sido un consuelo constante en este viaje académico

- Luz Borbor Suárez.

A mi mamá y mi abuelita, por su apoyo constante y por ser una fuente de inspiración. A mi familia en general, gracias por estar siempre ahí. Este logro es también de ustedes.

- Wilson Chaca Bravo

AGRADECIMIENTO

Queremos expresar nuestro más sincero agradecimiento a todas las personas e instituciones que hicieron posible la realización de esta tesis.

A la Universidad Estatal Península de Santa Elena (UPSE), por brindarnos la oportunidad y los recursos necesarios para llevar a cabo este proyecto. Su apoyo institucional ha sido fundamental en cada etapa de nuestra formación académica.

Al director de la Carrera el Ab. Víctor Manuel Coronel Ortiz, cuyo liderazgo y guía fueron significativos para orientar este trabajo en la dirección correcta, gracias por su visión y apoyo constante han sido invaluables.

A Diego Alejandro Borbor Suárez y a Erick Patricio Solano Bravo, por su valiosa ayuda en la organización y consecución de las entrevistas, su esfuerzo y dedicación fueron esenciales para obtener la información necesaria para esta investigación.

A nuestros tutores, el Ab. Wilfrido Wasbrum Tinoco y el Ing. Bolívar Suárez Lindao por su dedicación y orientación académica, puesto que con su experiencia y sugerencias mejoraron significativamente la calidad de este trabajo.

A los jueces de la provincia de Santa Elena, por ser parte de los entrevistados y compartir su tiempo y conocimientos, puesto que con sus perspectivas y experiencias enriquecieron significativamente este estudio.

A los trabajadores de las entidades privadas y a la Ab. Brenda Reyes, que amablemente accedieron a participar en las entrevistas. Su disposición y colaboración fueron primordiales para la recolección de datos y el desarrollo de este estudio.

A todos ustedes, nuestro más profundo agradecimiento por su apoyo y contribuciones, que hicieron posible la culminación exitosa de esta tesis.

ÍNDICE GENERAL

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD CARRERA DE DERECHO

CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023

Autores: Luz Borbor
Wilson Chaca
Tutores: Ab. Wilfrido Wasbrum
Ing. Bolívar Suárez

RESUMEN

La importancia de esta investigación radica en destacar los componentes esenciales del consentimiento, a través de este estudio, se ha identificado que muchas empresas no cumplen con estos requisitos al establecer contratos, lo que les permite obtener la autorización de sus clientes de manera ilegítima para el tratamiento y procesamiento de su información, una práctica que se ha vuelto prácticamente ubicua. Esto resalta la preocupante frecuencia con la que se vulneran los derechos individuales a la privacidad. A pesar de la existencia de leyes que protegen y regulan esta área, la aplicación adecuada por parte del Estado y la regulación por parte de sus autoridades son insuficientes. Esta brecha entre la legislación y su aplicación efectiva deja a los individuos en una posición vulnerable, ya que su derecho a la protección de datos no se encuentra efectivizado. En la primera fase de esta investigación se estableció la teoría, donde se crearon conceptos e ideas claves para ayudar a comprender el tema y el problema en cuestión. A continuación, se examina la ley sobre el consentimiento y uso de datos sensibles por parte de empresas privadas. Para realizar esta investigación se utilizaron diversos métodos como el análisis normativo y teórico. Estos métodos permitieron realizar un estudio de antecedentes de la literatura como doctrina jurídica, utilizando conocimientos reales. Además, se realizaron encuestas y entrevistas, cuyas respuestas se presentan en el capítulo 4, donde, a través del análisis cualitativo, se confirmó como se tiene una deficiente interpretación de la ley y los elementos de consentimiento que se deben cumplir al momento de la firma del contrato. Debido a que el uso de la ley se entendía más como una facultad y no como una regla de obligatorio cumplimiento. Lo que nos ha permitido concluir sobre la inaplicación facultativa por parte de las entidades privadas sobre la ley orgánica de protección de datos personales, sobre el consentimiento al entregar los datos sensibles, lo que vulnera el derecho a la protección de datos.

Palabras clave: Consentimiento, protección, datos, sensibles, empresas, informado

ABSTRACT

The importance of this research lies in highlighting the essential components of consent. This study has identified that many companies fail to meet these requirements when establishing contracts, enabling them to illegitimately obtain authorization from their clients for the treatment and processing of their information, a practice that has become nearly ubiquitous. This underscores the alarming frequency with which individual privacy rights are violated. Despite the existence of laws that protect and regulate this area, the state's enforcement and the regulation by its authorities are inadequate. This gap between legislation and its effective application leaves individuals in a vulnerable position, as their right to data protection is not being realized. In the first phase of this research, the theory was established, where key concepts and ideas were created to help understand the issue at hand. Following this, the law regarding consent and the use of sensitive data by private companies is examined. Various methods, such as normative and theoretical analysis, were used to conduct this research. These methods allowed for a background study of the literature, including legal doctrine, using real knowledge. Additionally, surveys and interviews were conducted, the responses to which are presented in Chapter 4. Through qualitative analysis, it was confirmed that there is a deficient interpretation of the law and the elements of consent that must be met at the time of contract signing. The law was understood more as a faculty rather than a mandatory rule. This has allowed us to conclude that private entities optionally apply the organic law on the protection of personal data regarding consent when providing sensitive data, thereby violating the right to data protection.

Keywords: Consent, protection, sensitive data, companies, informed

INTRODUCCIÓN

Los datos sensibles son fundamentales para la autonomía de una persona y guardan similitudes con los datos personales, sin embargo, su importancia radica en la forma que incide en la privacidad del individuo. Por esta razón, la protección de estos datos requiere una regulación más rigurosa por parte del Estado y las autoridades pertinentes. Es por ello que se lleva a cabo esta investigación como estudiantes de la Universidad Estatal Península de Santa Elena, en la carrera de Derecho, bajo el título "Consentimiento en el uso de datos sensibles y la Ley Orgánica de Protección de Datos Personales en el ámbito privado, 2023".

La relevancia de este proyecto reside en la elaboración de recomendaciones que fomenten una mayor regulación en la forma en que las empresas privadas solicitan el consentimiento para el uso de datos sensibles y llevan a cabo el tratamiento de esta información con sus clientes. El objetivo es mejorar las prácticas empresariales en relación con la gestión de datos sensibles, impulsando así un enfoque más ético en este ámbito.

En el capítulo I podremos encontrar todo lo relacionado con el problema de la investigación, como la necesidad de resaltar la importancia de los datos sensibles para la autonomía de la persona, la necesidad de una regulación más rígida en cuanto a la protección de esta información y la mejora de las prácticas empresariales en su gestión. Se resaltará el artículo 8 de la Ley Orgánica de Protección de Datos, que establece que el consentimiento debe ser libre, previo, específico, expreso, informado e inequívoco, cuyo planteamiento se establece en el objetivo general, así como el análisis de la definición y alcance de dichos requisitos para una autorización, y cómo se realiza la entrega y aplicación de estos según el conocimiento público.

En el capítulo II se encuentra el marco referencial, donde se estableció una amplia gama de doctrina bibliográfica para la elaboración del marco teórico. Aquí se sitúan conceptos básicos y teoría que ayudan a comprender mejor el tema y la problemática. Posteriormente, en el marco legal, se incluyó la legislación que se consideró más adecuada en relación con el consentimiento y el uso de datos sensibles por parte de las empresas privadas, como la Constitución, la Ley Orgánica de Protección de Datos y su reglamento, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, y tratados internacionales sobre derechos humanos, como el Pacto Internacional de Derechos Civiles y Políticos. Para el

correspondiente estudio del consentimiento, el derecho a la intimidad, la reserva de convicciones, los principios, el tratamiento de los datos sensibles y el consentimiento en cuanto al uso de medios electrónicos.

En el capítulo III se presenta el marco metodológico, donde se detalla el diseño de investigación cuya muestra es por conveniencia. Se establece la Constitución, la Ley de Protección de Datos, el reglamento y los tratados internacionales como base normativa. Además, se incluyen entrevistas a jueces de la Provincia de Santa Elena, representantes de entidades privadas y a una ciudadana, así como encuestas realizadas en la provincia de Santa Elena. Se utilizaron varios métodos, como el método exegético y el análisis histórico-jurídico, para extraer teoría de la doctrina, además del método de campo para realizar las encuestas mencionadas. También se presenta la operacionalización de variables.

En el capítulo IV, se presenta la evidencia en cuanto a los resultados y la discusión de las entrevistas y encuestas realizadas en el proyecto. Aquí se pudo verificar la idea a defender sobre la necesidad de que a las empresas privadas se le establezca una mayor regulación por parte del Estado, ya que la falta de desarrollo en los elementos que establecen para el consentimiento permite la vulneración del derecho a la protección de datos, por parte de estas.

CAPÍTULO I

1. EL PROBLEMA DE LA INVESTIGACIÓN

1.1 Planteamiento del problema

El internet ha sido visto como la invención más positiva de la humanidad para entretejer el tejido social y acortar distancias en el mundo, sin embargo, los actos del ser en su entorno digital se alejan de esta visión utópica.

Actualmente el uso de herramientas digitales, según lo explica el Foro Económico mundial (2023) las "aplicaciones de inteligencia artificial progresivamente más avanzadas, dispositivos interoperables de computación en el borde y del Internet de las cosas, y tecnologías autónomas" (pág. 42), permiten el correcto funcionamiento de la estructura social, por lo que desempeñaran un papel fundamental en el desarrollo de soluciones cuantitativas para las crisis del mañana, lo que implica recolectar datos, actividad que sucede todo el tiempo, ejemplos como abrir una cuenta en una red social, con datos personales reales o ficticios, hasta cuando se llena una encuesta en Google .

Se proyecta que para el 2025 el cibercrimen y la inseguridad sea de los mayores riesgos del mundo, además el ciberataque a estructuras físicas como lo puede ser el fichero o base de datos se encuentra como una de las cinco causas principales de la crisis global en el año 2023, dentro del mismo, el poder ejecutivo Ecuatoriano identifica en segundo puesto dentro de su top de principales riesgos a la desigualdad digital, según la encuesta de Percepción de Riesgos Globales (GRPS) que sustenta el informe de riesgos globales del (Foro económico mundial, 2023, pág. 82)

La humanidad se encuentra en la revolución digital, por ello es necesario estudiar las formas en que se recolectan los datos, el uso desmedido de datos sensibles y personales por empresas privadas causaría una vulneración al derecho de una vida privada libre de injerencias arbitrarias e ilegales prescrito en la Declaración de los Derechos Humanos (Asamblea General de las Naciones Unidas, 1948, págs. 4, art 12), esto por una falta de control del estado en los actos realizados entre el titular y el responsable del tratamiento, respecto del consentimiento al entregar los datos sensibles para que sean almacenados; generalmente estos actos no se realizan basado en los principios relativos de: tratamiento de manera lícita

y leal, recolección con fines determinados, explícitos y legítimos, datos exactos y si fuera necesario, actualizados que permitan al titular el acceso y decisión sobre su información y datos de este carácter.

Esto, lo causa un inexistente desarrollo de los elementos que la misma Ley Orgánica de Protección de Datos (LOPDP) personales proporciona como la *"*Manifestación de voluntad libre, previa, específica, expresa, informada e inequívoca, por la que el titular de los datos personales autoriza al responsable del tratamiento de datos personales a tratar los mismos*"* (Ley Orgánica de Protección de Datos Personales)

En la Constitución de la República del Ecuador (2008) en el artículo 66, núm. 19 establece que es un derecho de todos -la protección- de datos de carácter personal, que incluye tener acceso y tomar decisión sobre la información y datos de este carácter.

Las entidades que se encargan de realizar el tratamiento de datos sensibles presentan términos y condiciones para que sean aceptados por el titular, en esto se debería establecer cuál es el alcance otorgado, ¿sus datos serán usados con fines comerciales a un tercero o de marketing, almacenaran los datos de mensajería, o alimentaran una IA?, este alcance debe ser claro para que constituya uno de los elementos del consentimiento, sin embargo, la decisión facultativa de las empresas de como ejecutar esta disposición perjudica al ciudadano, no solo por el hecho de que se aprovechan del desconocimiento al consentir la entrega de datos sensibles, también por el uso desmedido de los contratos de adhesión que La Ley Orgánica de Defensa del Consumidor, define como: "aquel cuyas cláusulas han sido establecidas unilateralmente por el proveedor a través de contratos impresos o en formularios sin que el consumidor, para celebrarlo, haya discutido su contenido" (Asamblea Nacional, 2000)

La necesidad de las empresas que brindan un servicio basado en herramientas digitales, es la de acumular datos, para así poder generar una gran base o fichero de datos para fines comerciales, convirtiéndose los datos del titular en el bien más preciado de terceros, se valen de prácticas abusivas para obtener los datos sensibles a través de los contratos de adhesión, provocando una vulneración al derecho a la intimidad personal y familiar de la persona, al derecho al acceso a bienes y servicios (…) recibir información veraz sobre su contenido y características establecidos en la constitución art 66, numeral 20 y 25 y art 52. (Asamblea Nacional, 2008)

De acuerdo con la Constitución, el Habeas Data, entendido como el único recurso que le permite al titular ejercitar sus derechos, ya que permite "conocer el uso que se haga de ellos,

su finalidad, el origen y destino de la información personal y el tiempo de vigencia del archivo o banco de datos, (Asamblea Nacional, 2008), es común accionarlo contra las entidades públicas, sin embargo debería ser ejercida contra entidades privadas por igual.

Una de las causas, del problema que se presenta, es la falta de coerción del Estado contra las empresas privadas extranjeras que se encargan del tratamiento de datos, para que la base de datos que contenga la información del ciudadano ecuatoriano se encuentre en nuestro territorio, de esto se desprenda la obligación de establecer al responsable del tratamiento de datos y así reparar la vulneración a los derechos establecidos en la CRE y la LOPDP. La falta del representante legal del tratamiento de datos es una razón que mantiene vigente el problema de investigación.

La LOPDP, dispone que toda entidad pública o privada debe prestar un servicio de tratamiento de todo dato que sea almacenado en un fichero o base de datos, dicha acción técnica se define como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea, por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro (…)" (Asamblea Nacional, 2021).

El eslabón más débil de los datos son los sensibles, entendidos en la LOPDP, como los relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atención o puedan atentar contra los derechos humanos o la dignidad e integridad de las personas. (Asamblea Nacional, 2021)

María Luisa Pfeiffer (2008) reafirma lo expuesto sobre los datos sensibles "tiene que ver con los datos que afectan a lo más propio de la persona, podríamos decir a su intimidad" (pág. 25), y datos personales son los "que identifican o hacen identificable a una persona natural, directa o indirectamente, en el presente o futuro*"* (Ley Orgánica de Protección de Datos Personales, 2021).; esta norma y otras conexas, solo se enfocan en las instituciones públicas, ¿existe alguna que regule a las instituciones privadas?.

Si estas acciones, persisten en el tratamiento de datos sensibles, se constituirá un estado de indefensión para los ciudadanos, debido a la vulneración de los derechos respecto a la protección de datos qué, en una sociedad digital, se vuelve de carácter humano por su afección directa a la dignidad del ser, la propiedad, honra y privacidad. Los seres humanos

viven en una verdadera revolución digital, las inteligencias artificiales cambiaran la forma en cómo se desarrolla la vida; y la necesidad de desarrollar conocimiento en materia de derecho de datos, es esencial para abordar los desafíos que el mundo digital plantea, al derecho a la intimidad en relación directa con la protección de datos sensibles.

1.2 Formulación del problema

¿Las empresas privadas realizan ilícitamente el tratamiento de datos sensibles por la falta del consentimiento del titular en Ecuador en el 2023?

1.3 **Objetivos**

Objetivo general

Examinar los elementos del consentimiento en el uso de datos sensibles, mediante el estudio jurídico del artículo 66 numeral 19, 20 y 25 relacionado al derecho de protección de datos y la Ley Orgánica de Protección de Datos Personales en el Art. 8, complementando el estudio referente al reglamento (UE) 2016/679 del Parlamento Europeo, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos sensibles y la teoría del consentimiento contractual de Randy E. Barnett, que permitan la valoración de los elementos del consentimiento dentro de la Ley Orgánica de protección de datos enfocado en el ámbito privado.

Objetivos específicos

- Estudiar la evolución del derecho a la protección de datos, a través de la recopilación de información en relación a las generalidades del uso de datos y el desarrollo de las generaciones y el derecho a la protección de datos.
- Analizar la definición y alcance de los elementos del consentimiento en la entrega de datos sensibles, según lo establecido en el artículo 8 de la Ley Orgánica de Protección de Datos Personales, relativo al amparo de las personas físicas, en lo que respecta al tratamiento de datos sensibles y su libre circulación.
- Examinar la aplicación de la teoría del consentimiento contractual en los elementos que legitiman la entrega de datos sensibles, para el tratamiento de estos y el conocimiento de la población sobre la entrega de datos sensibles a las empresas privadas, a través de una encuesta a la población de los ciudadanos ecuatorianos

1.4 Justificación del problema

La investigación propuesta busca, mediante la aplicación de la teoría del consentimiento contractual de Bernett, que nos indica, que la confianza entre los sujetos que contratan radica en prima facie, el significado de las palabras o hechos que deben ser entendidos por ambos, para poder transferir derechos legítimamente, cuando el titular de los datos, firma de forma digital un contrato de adhesión para entregar los datos sensibles o personales, sin discutir o que se le explique el alcance o significado de los términos utilizados, contradice la teoría expuesta, elemento que le permitirá a los investigadores comprender la legalidad de las relaciones en el espacio digital, que radican en el consentimiento al entregar datos sensibles del titular, enfocados al uso en las empresas privadas.

Para lograr, los objetivos de la investigación, se acude al empleo de encuestas a ciudadanos, entrevistas a trabajadores privados relacionados al tratamiento de datos para medir el conocimiento sobre los elementos del consentimiento en las estipulaciones que componen los contratos para entregar sus datos sensibles, además de entrevistas para recolectar información de los jueces sobre su experiencia y conocimiento en la acción de habeas data como la única herramienta coercitiva que permite el derecho a la protección de datos que contiene nuestro ordenamiento jurídico.

Se investiga, el consentimiento en el uso de datos sensibles y la Ley Orgánica de Protección de Datos, en el ámbito privado porque es el único espacio que realiza el tratamiento de éstos, con fines lucrativos, acciones que van desde la obtención hasta el uso de los datos sensibles, lo que hace sus actuaciones más cuestionables, además de la percepción de inseguridad digital con respecto a nuestros datos en la internet, que se ve materializado en casos como el de Cambridge Analytica O Ecuador y Novaestrat, que filtraron datos que ellos habían obtenido contando con los requisitos de seguridad legalmente establecidos. De acuerdo a los objetivos de la investigación, se espera como resultado contribuir al desarrollo del conocimiento en materia de protección de datos, como un derecho humano de gran incidencia en la realidad y del que se espera grandes cambios con la llegada de la Inteligencia Artificial, que deben ser previstos para mantener el orden en la sociedad y así nuestra teoría a desarrollar sea una ayuda a investigaciones posteriores sobre una rama del derecho en construcción, como lo es el derecho informático.

1.5 Variables de investigación e idea a defender

Variables de investigación

V1: consentimiento en el uso de datos sensibles. VD

V2: la Ley Orgánica de Protección de Datos Personales en el ámbito privado. VI

Idea a defender

La falta de las reglas respecto a los elementos del consentimiento, en la entrega de los datos sensibles establecidos en el artículo 8 de la Ley Orgánica de Protección Datos Personales, permitiría a las empresas privadas a la vulneración del derecho a la protección de datos.

CAPÍTULO II

2. MARCO REFERENCIAL

2.1 Marco teórico

2.1.1 Generalidades de la protección de datos

Es esencia de la juridicidad de un problema social, que nazca de una necesidad, una serie de conductas especialmente lesivas que presenta la sociedad donde el Derecho se presenta como la fórmula para solucionar el conflicto, lo que nos lleva a conocer cómo surgió la necesidad de regulación jurídica en relación con el derecho de protección de datos, paralelamente analizar las condiciones técnicas materiales que han evolucionado la informática y el desarrollo normativo.

El expresidente Roosevelt en 1935, con afán de proteger los derechos de los trabajadores promulgo la Ley de Seguridad Social, donde se les otorgaba el beneficio a la jubilación, dentro de la misma ley, se estableció como una obligación del estado, la recolección de datos relativos si tenían seguro de asistencia médica, pensiones u otros beneficios sociales, esto se planteó como el primer reto en relación al tratamiento de datos lo que tiene estrecha relación con un neo derecho a la protección de datos, debido a la magnitud de la fuerza trabajadora que existía, la recolección de millones de datos presentaba su primer obstáculo, practicó la limitante técnica de las herramientas, logrando un cumplimiento parcial de esta disposición, mostrando la necesidad de desarrollo tecnológico para esta naciente labor.

El tan ansiado desarrollo tecnológico, se produce por la presión constante de satisfacer una necesidad y de una no menor aportación monetaria, para mejorar las técnicas que van desde: mejorar y perfeccionar las herramientas para la guerra, como por ejemplo, en 1943 se desarrolló Colossus, que tenía como objetivo descifrar en instantes los mensajes secretos de los nazis durante la Segunda Guerra Mundial, siguiendo esta línea bélica paralelamente en 1945, se desarrollaba en el laboratorio de Los Álamos la bomba atómica, el profesor John Von Neumann, crea lo que se considera el primer programa de ordenar, que realizaba una simple operación matemática y en el mismo año se establecen las bases teóricas de los ordenadores

Desde 1950, se dieron las primeras aplicaciones civiles de la informática, desde el uso comercial de los ordenadores, realizar predicciones electorales, el uso técnico empresarial para procesar datos contables, hasta que en 1962 en España el RENFE centraliza toda su informática en Madrid para gestionar datos relacionados al personal, estadística y contabilidad.

Probablemente, uno de los primeros autores en percibir este potencial peligro fue Arthur R. Miller, quien ya en 1969 reconocía los problemas legales relacionados con la privacidad que podía generar la informática. Del mismo modo, en 1972, A. Westin, publicó una monografía expresando preocupaciones similares. Tras analizar las principales bases de datos en Estados Unidos, concluyó su estudio alertando sobre posibles usos perjudiciales.

Este interés por los posibles daños de la informática se incrementó a medida que avanzaba la tecnología, especialmente cuando el uso del ordenador se generalizó, no solo entre empresas e instituciones, sino también entre particulares.

Así, se comenzó a regular jurídicamente este ámbito, evidenciando el peligro que implicaba para los derechos fundamentales. Curiosamente, la primera norma sobre protección de datos no surgió en Estados Unidos, a pesar de ser pionero en el desarrollo y aplicación de los ordenadores. En cambio, fue en Europa, específicamente en el estado alemán de Hesse, donde se promulgó la primera ley limitando el uso de la informática, la Datenschutz del 7 de octubre de 1970, seguida por la Data Lag de Suecia en 1973.

Estas primeras normativas no surgieron de la nada, sino que representaron la materialización jurídica de propuestas previas de órganos de la Unión Europea. En 1967, el Consejo de Europa, creó una comisión consultiva para estudiar las tecnologías de la información y su posible impacto en los derechos humanos. Este trabajo culminó en la Resolución 509 de 1968 de la Asamblea del Consejo de Europa, que destacaba la posible confrontación entre derechos humanos y los avances científicos y técnicos.

En 1973, el Comité de Ministros del Consejo de Europa emitió una resolución recomendando a los miembros del Estado, tomar precauciones para evitar el uso indebido de datos personales en bancos de datos privados. Un año después, publicó otra resolución similar, pero enfocada en los bancos de datos públicos. En 1974, Estados Unidos aprobó la Privacy Act, el texto más completo y estructurado hasta entonces, que se convirtió en el precursor de futuras normativas sobre protección de datos personales.

Tecnológicamente, lo mejor estaba aún por llegar. En 1965, L. Roberts y T. Merril conectaron por primera vez dos ordenadores a través de una línea telefónica, demostrando la facilidad de transmisión de datos y dando origen a ARPANET. Para 1970, ARPANET ofrecía servicios de correo electrónico y transferencia de archivos dentro de Estados Unidos, y en 1973, logró las primeras conexiones internacionales. Inicialmente, se conectaban ordenadores individuales, pero posteriormente se interconectaron redes de ordenadores. Según De Andrés Blasco, esta situación reveló problemas de diseño inicial: ARPANET estaba concebida para interconectar ordenadores, no redes de ordenadores.

ARPANET, fue mejorada técnicamente, permitiendo la conexión de ordenadores de diferentes fabricantes y destacando sus enormes posibilidades, basadas en la capacidad de transmitir datos a través de líneas telefónicas. Tanto ARPANET como INTERNET funcionan mediante una serie de protocolos, es decir, reglas que estandarizan procedimientos repetitivos. El 1 de enero de 1983, el protocolo NCP fue sustituido por TCP/IP, separándose la parte militar (Milnet) y dando lugar a INTERNET, que coexistió con ARPANET hasta 1990. Un año después, surgió la World Wide Web tal como la conocemos hoy. La popularización de su uso trasladó la informática del ámbito técnico al centro de la vida ciudadana, convirtiéndola en una herramienta de trabajo y un medio global de intercambio de información y comunicación. Sin embargo, a pesar de ser un ejemplo de colaboración y una valiosa herramienta social, pronto se confirmó la necesidad de una regulación para evitar la vulneración de derechos fundamentales, lo que requería la intervención del Estado a través de la legislación.

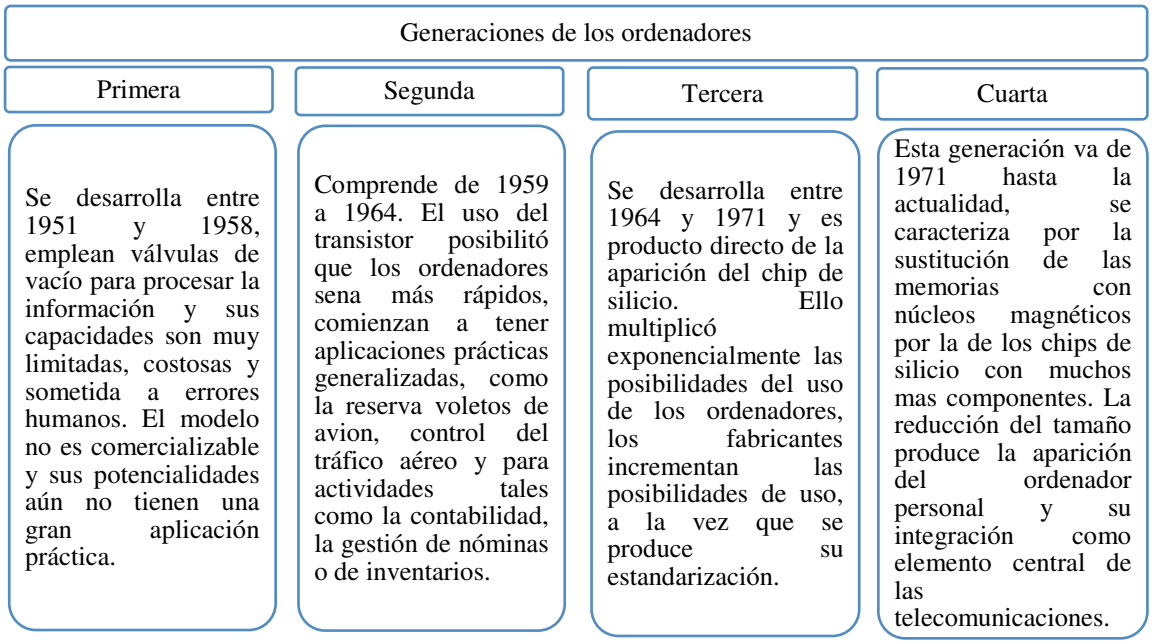
El problema ahora, con la globalización del uso de la Red, es que el Estado tiene dificultades para controlar ciertas actividades, ya que su actuación está limitada por el alcance de sus propias leyes. Como se puede ver, cualquier avance tecnológico que implique un uso social termina requiriendo intervención jurídica. En este caso, la existencia de un espacio virtual transfronterizo demanda una regulación universal para la informática y el uso de la Red, lo cual plantea numerosos desafíos.

2.1.2 La protección de datos y las 4 generaciones

Puede parecer lógico, hacer coincidir las denominadas cuatro generaciones en la evolución de los ordenadores, en las comúnmente llamadas también concepciones en las leyes de protección de datos. Conviene no obstante analizar estas evoluciones para constatar su no

coincidencia, si bien hay en ellas una lógica dependencia, dado que hasta que no se constata la posibilidad técnica, y ésta se generaliza, no surge la necesidad jurídica.

GRÁFICO 1 GENERACIONES DE LOS ORDENADORES



Elaborado por: Luz Borbor y Wilson Chaca Fuente: Rebollo Delgado, L.

2.1.3 Del derecho a la protección de datos

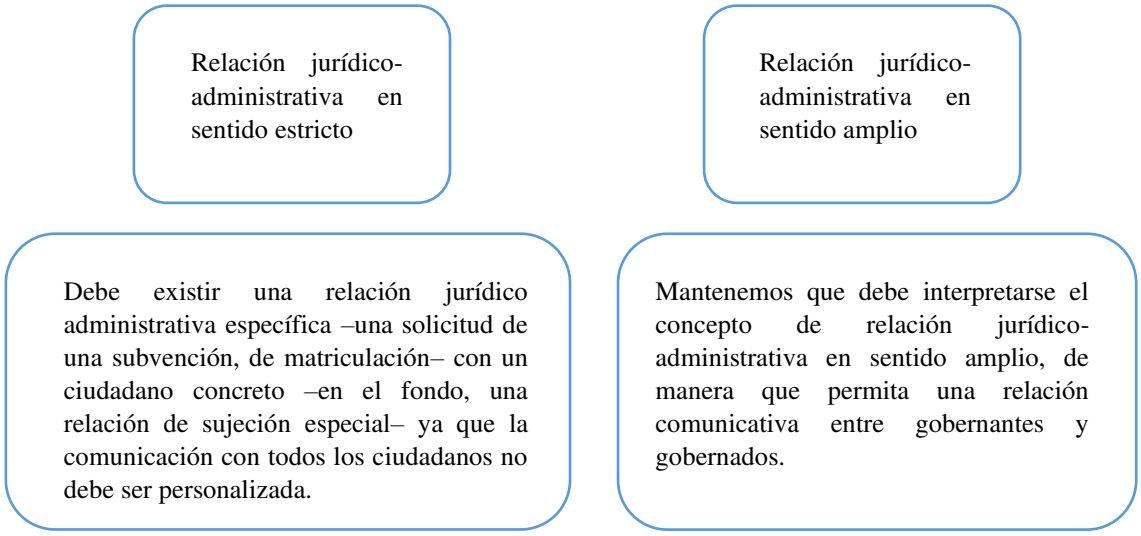
Los estados reconocen en la actualidad, la exigencia fundamentalista de establecer como un bien jurídico la protección de la identidad individual humana en un escenario digital; que comúnmente se puede expresar en pequeños cuadros (datos personales) que conforman un mosaico, que podríamos denominar identidad y a su vez nos permitiría identificar a ese humano en una base de datos qué, como objetivo, tiene la cuantificación objetiva de las características humanas.

Este reconocimiento del derecho humano a la protección de datos como una perspectiva de un humano digitalizable, exige del estado una actividad administrativa que garantice su estricto cumplimiento, dentro de las relaciones que establece una persona o grupo de personas entre sí, de forma privada, o los ciudadanos y extranjeros entre el estado, lo que en el fondo justifica la existencia de esta entelequia centralizada y con capacidad coercitiva de hacer cumplir lo que se encuentra pactado socialmente dentro de la constitución de cada estado, disposiciones expresas en esta materia dentro de la base estructural (Constitución) de los estados, demuestra que se encuentran a la vanguardia de las necesidades de una sociedad internacionalizada.

La actividad administrativa, tanto en las funciones públicas de soberanía, como en el uso privado de los datos personales, exigen frecuentemente el tratamiento de datos personales, por lo que se vuelve una necesidad, establecer un conjunto de reglas claras, para quienes disponen de información personal o sensible, a través del cumplimiento de disposiciones que limiten sus conductas, naciendo esta responsabilidad de la firma del consentimiento informado, donde se define que se usara únicamente para una finalidad administrativa legítima, por lo que en un principio fueron recogidos, sin que su actividad material sea distinta de la que se había pactado o establecido, como objetivo particular de la entidad pública.

En el estudio introductorio a la protección de datos se puede comprender a la relación jurídica administrativa que da origen al tratamiento de datos "de manera estricta o de manera amplia" (Rebollo Delgado, L, 2008, pág. 19).

GRÁFICO 2 TIPOS DE RELACIONES JURÍDICAS



Elaborado por: Luz Borbor y Wilson Chaca Fuente: Rebollo Delgado, L.

Esta distinción, nos permite comprender como funciona y se diferencia el sector privado del público, mientras en la práctica una serie de disposiciones normativas que generan derechos, produzcan efectos jurídicos y cuyo incumplimiento pueda sancionarse a través de la jurisdicción competente, se aplican como engranaje en el sector público, por el hecho de ser el estado que garantiza la seguridad jurídica y así justifica el uso de los datos sensibles para, cumplir con las garantías normativas y el desarrollo de políticas públicas, mientras que las entidades privadas a través del uso de herramientas jurídicas, como lo es el contrato puede tratar los datos sensibles de los usurarios, previo consentimiento y para un fin único, este

instrumento que sirve para establecer una relación jurídica debe ser específica y no debe contener fines múltiples, ya que la responsabilidad debe ser delimitada al tratarse del manejo de datos sensibles (Rebollo Delgado, L, 2008).

Así, entiende el sujeto que contrata con la empresa, que tratara sus datos sensibles, que a través del consentimiento sesiona o transfiere su información dentro de una plataforma para un uso específico, por ejemplo puede ser destinatario de mensajes que busquen venderle un servicio o producto que según el análisis de sus datos la convierte en potencial cliente, también se debe entender claramente que la interacción con la plataforma tiene también el fin de alimentar una inteligencia artificial o un fichero de datos externo que la podría identificar como un sujeto con ciertas características especiales inherentes a su identidad, al juntar todos los datos que se han aportado y el abanico de oportunidades podría crecer al infinito según las necesidades futuras.

Con esta tesis, se sostiene que la administración en sentido amplio se convierte en un potencial peligro debido a la amplia gama de usos que se le pueden dar a los datos, por ello el consentimiento tiene que contener disposiciones normativas específicas, que legitimen el tratamiento, generen derechos, produzcan obligaciones y si se llegan a violentar se cuente con las sanciones y el proceso adecuado a seguir (Rebollo Delgado, L, 2008, pág. 20).

Constituye un derecho que ha sido elevado a la calidad de humano, que ha sido reconocido en la constitución y tratados internacionales como la Declaración de los derechos humanos, el cual dota a todos los ecuatorianos y extranjeros dentro de nuestro territorio de la capacidad para tomar conocimiento de todos los datos que conformen los ficheros de datos, la finalidad del uso de esa información y la exigencia de su corrección, actualización y eliminación.

La modernización y digitalización de la identidad nos ha demostrado que la "recopilación, procesamiento, almacenamiento y transmisión de datos personales, se ha venido convirtiendo sobre todo en una lucrativa actividad" (Garcia Falconi, 2000, pág. 7), esto en la actualidad es un hecho, y la evolución tecnológica facilita las formas de transaccionar por un fichero o base de datos, de forma legítima o ilegal, por ejemplo, el diario EL COMERCIO el uno de octubre del dos mil diecinueve público un artículo, donde nos explica cómo se comercializa con facilidad la información de las familias ecuatorianos en la Deep web, por un valores que oscilan desde los mil dólares hasta los treinta mil.

Según el orden jerárquico, establecido en el artículo 425 de la Constitución de la República del Ecuador, la Ley Orgánico de Protección de Datos Personales, es el conjunto de reglas

específicas para regular todo lo relacionado a los datos personales, a todas las etapas del tratamiento de datos; lo que tiene íntima relación con el derecho a la privacidad y a la protección de datos, e impide a la entidad encargada del tratamiento "la intromisión perturbador y la inadecuada difusión de datos procesados" (Garcia Falconi, 2000, pág. 8), estableciendo sanciones por su incumplimiento.

Partiendo del principio democrático de que el poder ha de estar so- metido al Derecho, es fácil deducir una solución incontestable a esta problemática social moderna, sometamos a norma la actividad susceptible de lesionar derechos, la realice el Estado o los particulares. Esta solución es eminentemente teórica, y a la vez está exenta de todo inconveniente, tanto funcional, como jurídico y social.

El entendimiento de la fundamentación de la protección de datos requiere un inexorable acercamiento al derecho a la intimidad, que se constituye en la construcción jurídica central, entorno a la cual los ordenamientos jurídicos modernos soportan la defensa de los derechos de los ciudadanos y no sólo frente a la informática, sino también a cualquier ingenio tecnológico.

El término jurídico de intimidad es relativamente nuevo y ha experimentado un desarrollo notable, el cual se puede dividir en tres concepciones distintas:

a) Concepto objetivo de derecho a la intimidad: Este concepto se basa en la definición del término "intimidad" como la zona personal y privada de una persona o familia. La teoría alemana de las esferas concéntricas ilustra este concepto dividiendo la privacidad en varios niveles: lo íntimo en el centro, seguido por lo familiar, lo secreto o confidencial, y finalmente lo público. Cada individuo configura estas esferas según sus preferencias personales.

b) Concepto subjetivo de derecho a la intimidad: Este concepto se relaciona con el "derecho a la autodeterminación informativa". Según una sentencia del Tribunal Constitucional alemán de 1983, sobre la Ley del Censo y de Población, se establece que cada persona tiene el derecho a decidir cuándo y en qué medida revelar información sobre su vida personal. Así, la intimidad se convierte en un ámbito que la persona controla, decidiendo, qué información compartir y manteniendo el control sobre la misma. El derecho a la intimidad protege contra intrusiones no deseadas, y, asegura que la vida privada y familiar quede excluida del conocimiento público sin consentimiento.

c) En la teoría del mosaico, se presenta otro enfoque del derecho a la intimidad. Esta perspectiva es una doctrina más reciente, concebida como una respuesta a la necesidad de proteger la privacidad del individuo frente a las amenazas generales que plantean los avances tecnológicos, especialmente la informática. Esta teoría fue propuesta por Madrid Conesa, quien sostiene que la teoría de las esferas no es válida, dado que hoy los conceptos de lo público y lo privado son relativos, pues existen datos que a priori son irrelevantes desde el punto de vista del derecho a la intimidad, pero que unidos unos con otros, pueden servir para configurar una idea prácticamente completa de cualquier individuo, al igual que ocurre con las pequeñas piedras que forman un mosaico, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado. (Rebollo Delgado, L, 2008)

La concepción del derecho a la intimidad, que combina las definiciones objetiva y subjetiva, resulta la más adecuada tanto para entender este derecho como para satisfacer las necesidades de nuestro ordenamiento jurídico. Esta visión integral responde a la evolución del derecho a la intimidad, que ha ampliado sus límites y configuración. Originalmente concebido como un derecho de defensa y exclusión, ha evolucionado hacia un derecho que permite al individuo controlar y gestionar lo que le afecta. En esencia, el derecho a la intimidad se refiere a un espacio personal de libre disposición, cuyo pleno ejercicio se da en relación con otros, tanto para hacer valer este derecho como para compartirlo.

No obstante, el concepto de derecho a la intimidad no puede ser estático, dado su componente subjetivo. Este derecho varía de una persona a otra, de un grupo a otro y de una sociedad a otra, influenciado por factores como la edad, la cultura, la educación y la comunidad. Entre estos, el factor más determinante es la configuración social que una sociedad concreta realiza en un momento dado. El derecho a la intimidad se fundamenta inexorablemente en la dignidad humana y el libre desarrollo de la personalidad. Incluye pretensiones personales (lo privado), elementos sociales que condicionan esta autonomía (lo público) y la disposición voluntaria de un ámbito específico por parte del titular del derecho.

Estas circunstancias se sitúan en un contexto temporal y social que influye decisivamente en la configuración del derecho a la intimidad. Además, es necesario extender la protección de la intimidad privada al ámbito público, permitiendo que el individuo conozca y controle lo que afecta a su intimidad, incluso fuera de su esfera privada. Este control y

autodeterminación son esenciales para garantizar la libertad y la configuración activa de la propia intimidad.

El derecho a la intimidad protege la autorrealización del individuo, garantizando que ciertos aspectos de su vida permanezcan desconocidos y que el individuo controle la información que otros conocen sobre él. La intimidad actúa como un elemento de desconexión social, directamente relacionado con la dignidad humana y el libre desarrollo de la personalidad. La capacidad de controlar lo que afecta a la intimidad personal está intrínsecamente vinculada a la libertad.

2.1.4 Derecho fundamental a la protección de datos personales como derecho diferente y autónomo del derecho a la intimidad

En una sociedad en constante avances tecnológicos e intercambio de información es importante proteger el derecho a la intimidad para preservar la dignidad humana permitiendo a las personas vivir sin que su privacidad sea invadida, respetando la autonomía de los individuos a decidir qué hacer con su información. El derecho a la intimidad protege la esfera más íntima y personal de un individuo, esto incluye aspectos como la privacidad en el hogar, la correspondencia, la inviolabilidad de las comunicaciones, entre otros.

> Esto lo confirma (Sabater, Carmen, 2018, pág. 46) en su crítica vidas de cristal; análisis del derecho a la intimidad en la sociedad de la información donde indica que es un derecho complejo que comprende y se vincula a su vez con varios derechos específicos que tienden a evitar intromisiones extrañas en estas áreas reservadas del ser humano, como son:
>
> - El derecho a la inviolabilidad del domicilio,
> - El derecho a la inviolabilidad de correspondencia,
> - El derecho a la inviolabilidad de las comunicaciones privadas,
> - El derecho a la propia imagen,
> - El derecho al honor,
> - El derecho a la privacidad informática,
> - El derecho a no participar en la vida colectiva y a aislarse voluntariamente,
> - El derecho a no ser molestado.

Estos derechos encuentran su conexión directa con la protección de datos personales, ya que el resguardo de la privacidad se ve afectado por la recopilación, tratamiento y uso de la información personal.

La protección de datos personales se refiere a la correcta regulación -control- y garantía de que la información personal y en especial datos sensibles de un individuo no sea utilizada de forma incorrecta o indebida, protegiendo de este modo la confidencialidad, tomando medidas para prevenir que el acceso a esta información no recaiga en personal no autorizado o ajeno al tratamiento; y la autonomía del sujeto, dando paso al consentimiento informado, en que la persona debe ser consiente de cómo serán utilizados sus datos y que este de su aprobación de forma libre, previa, específica, expresa, informada e inequívoca, aplicando los elementos de este, dando a entender que pueden decidir qué información desean proporcionar, para qué propósito y a quién.

Estando en la era digital la privacidad es un privilegio de pocos, ya que no todos pueden cuidar que sus datos no sean utilizados con un fin diferente para el que se ha consentido, especialmente si se habla de entidades privadas que no están correctamente reguladas en la legislación, además de que la comprensión técnica sobre estos temas es una ventaja de algunos. La capacidad de poder manejar la manera en que de recopilan, almacenan y utilizan los datos personales es esencial para conservar la autonomía y dignidad de los individuos

De acuerdo con (Garriga Dominguez, A) en su libro nuevos retos para la protección de datos personales En la Era del Big Data y de la computación ubicua menciona que: El ciudadano de un Estado social de Derecho no tiene un poder absoluto e ilimitado sobre sus datos personales, al ser una persona que se desenvuelve en una comunidad social en la que la información y la comunicación resultan imprescindibles. Por estas razones, “la información, aún aquélla que se refiere a datos personales, ofrece una imagen de la realidad social que no puede ser patrimonio exclusivo del interesado” (Garriga Dominguez, A, pág. 94)

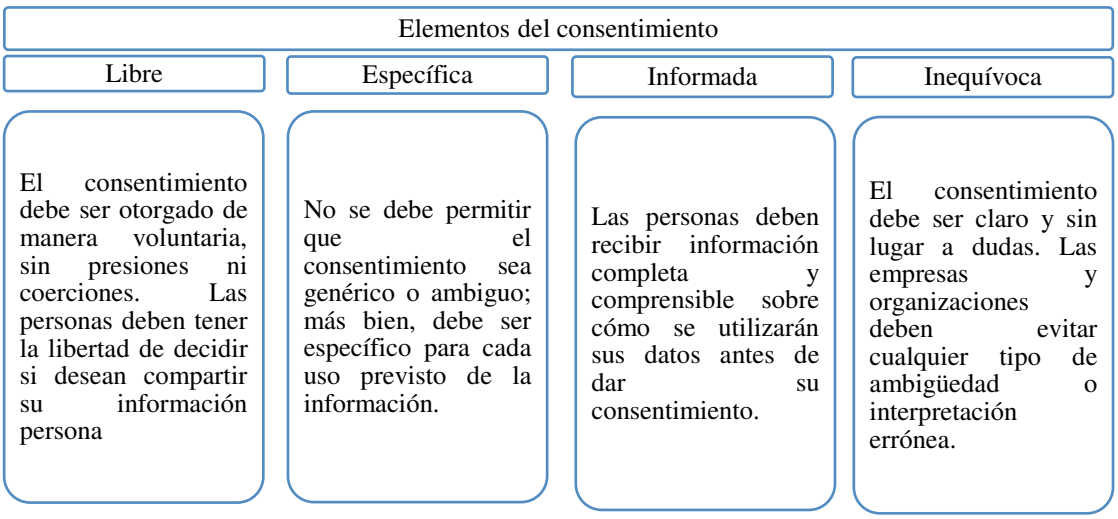
En la actualidad el manejo de datos personales y sensibles por parte de las empresas privadas en donde no está completamente regulado plantea retos tanto éticos como legales, ya que la falta de ordenamiento da a entender aparentemente para dichas entidades que se les otorga una licencia para el usos indiscriminado de información personal, discrepando con Garriga Domínguez, ya que esta información debe ser exclusivamente del interesado y atentaría contra su autonomía el no poder decidir qué hacer y qué no con estos datos. En consecuencia, el consentimiento y cada uno de sus elementos debería ser una pieza fundamental en este tiempo en que las tecnologías tienen un uso principal en gran parte de las acciones que se realizan.

De este modo, el amparo al derecho a la intimidad actúa como un valor importante en la sociedad actual, con los constantes avances en cuanto a tecnología y la transferencia de información, protegiendo la privacidad no solo mantiene la dignidad humana intacta, sino que permite a los individuos tener una vida fuera de luces que no sea perpetrada por individuos fuera de esta.

Este derecho encuentra una conexión con otros derechos específicos, como la inviolabilidad del domicilio, la propia imagen, el honor, la privacidad informática y el derecho a no ser molestado. Todos estos se entrelazan con la protección de datos personales, por ello el tratamiento adecuado de estos datos se vuelve importante, y de especial cuidado, valorando su autonomía en la toma de decisiones respecto a su información y la confidencialidad.

El consentimiento se vuelve un componente importante en la protección de datos personales, aunque también es esencial comprender y reconocer que en la realidad las personas no tienen un control absoluto sobre sus datos privadas, porque forma parte de una sociedad donde la información y comunicación son vitales. Entonces, habría que buscar un equilibrio que garantice la protección de datos personales sin comprometer la autonomía de los individuos dentro de las empresas privadas con escasa regulación.

GRÁFICO 3 ELEMENTOS DEL CONSENTIMIENTO



Elaborado por: Luz Borbor y Wilson Chaca

Examinando que estos son los elementos que un consentimiento debería tener según la normativa ecuatoriana, se pone a consideración que se requiere de un control más exhaustivo

para la respectiva revisión de su aplicación, ya que es un tema que no se puede tomar a la ligera, ya que la intimidad es considerada un derecho fundamental.

2.1.5 El Consentimiento como fundamento básico del contrato: Una Perspectiva Teórica

Los contratos son acuerdos que son realizados entre dos personas o más (también instituciones), con el objetivo de obtener un beneficio a cambio, como bienes, dinero o servicios, dentro de estos los individuos expresan su voluntad, creando de esta manera una relación legal con el contrario.

Para Randy E. Barnett en una obligación contractual la titularidad de derechos en los individuos delimita lo que pueden hacer con estos y les permite estar libres de interferencias para ejercerlos, por lo que, al momento de intercambiar, vender o donar, los derechos sobre un objeto se transfiere la titularidad de manera voluntaria, por lo que existe existe una relación de dependencia entre una obligación contractual y la voluntariedad del individuo.

La relación que se establece radica en el hecho de que la base de muchas obligaciones contractuales es la transferencia voluntaria de derechos entre las partes involucradas. Es decir, cuando se asume un compromiso contractual, se basa en una decisión voluntaria de ceder o intercambiar derechos, lo que determina la validez y la legitimidad de la obligación resultante.

> "Derecho contractual es el que se encarga de la exigibilidad de las obligaciones que surgen de la transferencia válida de titularidades que ya alguien poseía, y esta diferencia es la que hace al consentimiento un pre- requisito moral para la obligación contractual." (Randy E Barnett, 2004, pág. 64)

Dentro del derecho contractual se hacen exigibles las obligaciones que salen a flote una vez que se realiza una transferencia válida de la titularidad de un derecho, es decir que se hacen bajo los lineamientos legales, destacando que el consentimiento de ambas partes es un requisito moral básico y fundamental para que esta exista.

En resumidas cuentas, el consentimiento pasa a ser una de las bases que rige un contrato, ya que solamente siendo voluntario este se convierte en legal y ético. Se puede destacar que es un componente que determina lo que es una transferencia válida con lo que no, en un sistema de titularidades. La exigibilidad legal de dichas obligaciones encuentra su justificación en la

ética por que el promitente realiza actos que son voluntarios y estos comunican su intención de iniciar una responsabilidad.

2.1.6 El consentimiento como un derecho

El derecho fundamental a la protección de datos se sostiene en "el consentimiento, por una parte, y los derechos de los interesados por otra" (Rebollo Delgado & Mercedes Serrano, 2008, pág. 127). El consentimiento se manifiesta como una las máximas libertades dentro de un país democrático, facultando al individuo de plena libertad para decidir sobre sus datos, existiendo ciertas excepciones establecidas dentro de la normativa, el segundo elemento se refiere a el conjunto de derechos que tiene el individuo para ejercer el derecho a la acción para la protección a los datos, tema que es profundizado en el habeas data.

Este derecho al consentimiento para el tratamiento de datos debe cumplir con ciertos requisitos o complementos inherentes, como lo es la capacidad para establecer una relación jurídica con el ente de recogida u oponerse a ella en cualquier instancia, otro elemento es el conocimiento que le permite saber en todo momento al individuo, de quien dispone y que uso le están dando a sus datos.

La información es esencial para otorgar el consentimiento, se constituye como un elemento intrínseco que según la circunstancia debe presentarse de forma clara, así lo define y reafirma la Carta de derechos Fundamentales de Niza del año 2000 en el "Art 3. H) al aludir a la voluntad libre, inequívoca, específica e informada" (Rebollo Delgado & Mercedes Serrano, 2008, pág. 128). La información es esencial para que los otros elementos se materialicen en cualquier acuerdo donde el individuo faculte a un tercero para realizar la recogida y el tratamiento en general de los datos sensibles, no puede existir el consentimiento sin uno de estos elementos y las reglas deben ser claras para establecer, definir o conceptualizar de una forma transversal y clara que es inequívoca, especifica y voluntad libre para el legislador y por qué son tan necesarios estos elementos.

2.1.7 Libertad en el consentimiento

Desde el punto de vista del derecho civil, la libertad de consentimiento significa la capacidad de una persona de expresar su voluntad de forma libre y no coercitiva, esta libertad es necesaria para garantizar que las acciones y acuerdos reflejen verdaderamente las intenciones de las partes involucradas "Libertad en la prestación de consentimiento, que

alude a la ausencia de alguno de los vicios que afectan a la voluntad según el Código Civil" (Rebollo Delgado & Mercedes Serrano, 2008, pág. 128). En estricta correlación la libertad se asocia con la voluntad y si esta no cuenta con alguno de los vicios del consentimiento, que según nuestro código civil en el Art 1467 son el error, fuerza y dolo.

Cuando se pretenda recoger en un contrato de términos y condición la sesión de datos sensibles recaería en error, ya que no es el acto contractual pertinente para la recogida de datos que serán utilizados para la venta o para el uso lucrativo de la entidad, entiéndase el desarrollo de software, quizás podríamos definir al contrato útil como una permuta o compraventa, según lo que se reciba y lo que genere réditos para el tercero que brindara el tratamiento a los datos sensibles.

La fuerza como tradicionalmente se conoce no considero que se aplique en estos casos sin embargo, no se descarta en acasos excepcionales, lo que si se presenta como una complejidad es comprender hasta qué punto el monopolio de las apps o programas y por ende su uso completamente gratuito, se podría considerar una fuerza, ya que la única condición para que se pueda usar apps esenciales para el desarrollo en la era digital, es que se acepte los términos en los que esa entidad quieren que aportes tus datos y en los que ellos deben de tratar los datos, sin que nos quede claro cuál será su fin y alcance del uso, evaluar el dolo en estas causas puede ser muy subjetivo, por ello contar con el derecho a la protección de datos es mantenerse a la vanguardia de las necesidades sociales.

2.1.8 La especificidad e información en el consentimiento

Lo especifico en el consentimiento se relaciona al objetivo del tratamiento concreto, conocer con claridad cuál es la finalidad del uso de los datos personales o sensibles, que debe ser explicado de tal forma que no quede duda, todos los elementos que componen ese fin deben ser explícitos y es en este elemento que se evalúa la legitimidad del tratamiento por lo que se parte de un análisis previo de la normativa para conocer si ese usuario pudiere entregar su consentimiento o esa entidad está facultada para solicitar el consentimiento.

La información como elemento influye como eje transversal en el resto de componentes del consentimiento, debido a que se presenta de forma previa como toma de contacto con el individuo, teniendo como punto de partida una estrecha relación con la especificidad del

tratamiento, junto con la exigencia de la existencia de una comunicación asertiva y sencilla para que así se pueda tomar una decisión libre e inequívoca.

2.1.9 El consentimiento inequívoco

Se entiende que el consentimiento debe ser explícito y no se puede comprender la existencia de este por la mera realización de actos del individuo, en interacción con el tratamiento, es decir que no se admite el presunto consentimiento, ergo, se necesita la afirmativa del consentimiento al ceder los datos personales o sensibles en los supuestos que la ley lo permita.

El consentimiento tácito, una práctica común que es completamente ilegal, sin embargo, tiene sus excepciones, que cumpla con lo inequívoco, se debe dar un tiempo prudente que en legislaciones internacionales es de 30 días, para que la entidad se comunique con el individuo con el fin de que otorgue el consentimiento y si este presenta una inacción a la negativa del tratamiento implicaría el mismo, que el individuo tiene pleno conocimiento inequívoco sobre el uso de sus datos.

Existe otro tipo de consentimiento que relaciona el derecho a la información con el de protección de datos, esto se da en los casos donde el interesado no sea el que proporciona los datos y tampoco haya consentido su recopilación, primero se debe subsanar la falta de certeza al conocer el tratamiento y uso de los datos, que solo se puede lograr entregando la información necesaria según la necesidad, por lo que el individuo tiene el derecho a la información y la entidad se encuentra en la obligación de proporcionarla en los términos expuestos, en este caso la revocatoria debe ser inmediata sin causa justificada si se presenta la negativa al tratamiento.

2.1.10 Revocatoria del consentimiento

En los actos donde prima la voluntad se demuestra en esencia la libertad, por ello es que la revocatoria del consentimiento tiene sentido, ya que entregar los datos es un acto en donde prima la voluntad libre; La revocatoria implica de forma superficial que ya no se desea que los datos formen parte del tratamiento, siendo necesario su retirada de la base de datos o ficheros, un entendimiento más técnico nos dice que la revocatoria se completa con “la cancelación de los datos sometidos a tratamiento, de manera que el dato quede bloqueado y se impida su utilización posterior” (Rebollo Delgado & Mercedes Serrano, 2008, pág. 130).

2.1.11 Los datos sensibles y la confidencialidad en la era de las Tics.

En la era de las TIC (Tecnologías de la Información y la Comunicación), internet se ha integrado profundamente en la vida cotidiana de las personas. Sin embargo, esta integración también ha traído consigo un debilitamiento en el ejercicio del derecho a la privacidad. Internet introduce nuevos riesgos asociados con el tratamiento inadecuado de datos personales y sensibles, exponiendo a los usuarios a potenciales vulnerabilidades. Es necesario establecer una clara diferencia entre datos personales y datos sensibles.

GRÁFICO 4 DIFERENCIACION ENTRE DATOS PERSONALES Y DATOS SENSIBLES

Datos personales	Datos sensibles
• Podemos considerar como dato personal toda información sobre una persona física (o jurídica) que permita su identificación de manera directa o indirecta. Como ejemplos podemos mencionar: las huellas dactilares, la dirección domiciliaria, la pertenencia a un partido político, las creencias religiosas, entre otros.	• Debemos empezar afirmando que la información sensible permite conocer características que forman parte del "núcleo de la personalidad y dignidad humanas". Entre estos datos destacan: el origen racial, los datos referidos a la ideología, religión o creencias, los datos relativos a la salud, la orientación sexual, entre otros.

Elaborado por: Luz Borbor y Wilson Chaca Fuente: Karin Castro Cruzatt

Se puede decir que existe una diferenciación entre estos dos conceptos, los datos personales son aquellos que pueden hacer que una persona física sea identificable como nombres, números de identidad, emails, números de teléfonos, etc. Mientras que los datos sensibles es información más íntima, aquellos que pueden generar una vulnerabilidad para el titular los cuales incluyen información sobre la salud, orientación sexual, afiliación sindical, creencias religiosas, filosóficas o políticas, datos biométricos.

Ambos guardan una relación directa e innegable con la privacidad y la intimidad tanto personal como familiar de los individuos, pero los datos sensibles son de un área más -intima- porque su divulgación puede generar una exposición a discriminación, estigmatización y daños directos o indirectos al sujeto, por tanto, podría significar una amenaza para este.

Por ello, cuando el individuo brinda esta información, tiene que ser de forma voluntaria y con la certeza de que estos serán usados con mucha confidencialidad por una persona o entidad responsable y que no sean vendidos a un mejor postor por grandes cantidades de dinero.

De acuerdo con María Luisa Pfeiffer, en su artículo sobre el Derecho a la privacidad - Protección de los datos sensibles nos indica que:

> La confidencialidad sería la actitud o comportamiento de respeto, de silencio, de reserva, que pide el hecho o dato íntimo o privado, en la persona que lo conoce. Secreto frente al secreto es la respuesta adecuada al carácter íntimo o privado de ciertas revelaciones. (Pfeiffer, María Luisa, 2008, pág. 27)

Cabe destacar que la confidencialidad en los contratos en donde se encuentren implicados los datos sensibles que son personalísimos del sujeto, implica que se debe llevar con la máxima discreción y respeto posible, por esta razón los responsables del tratamiento tienen que ser personas totalmente capacitadas que puedan guardar silencio (no divulgar estos daros a terceros que no están autorizados) sobre dicha información, conservando así la integridad de las personas

Por otro lado, se extienden de un modo inimaginable las plataformas en línea que también realizan una recolección de información e intercambian datos sensibles a partir de registros en algoritmos o comercio electrónico, generando preocupación sobre la seguridad al no tener certeza de cómo es el tratamiento de información en dichas aplicaciones y sin una regulación adecuada como garantía de que no habrá un robo de identidad o situaciones peores.

De lo dicho, se desprende que la protección de los datos sensibles y personales tienen como factor de gran importancia la confidencialidad y el respeto por parte de la persona encargada del tratamiento al no transferir la información íntima y especialmente delicada que podría exponer al titular a algún tipo de discriminación o daños a su integridad.

La voluntad del individuo para otorgar información de este carácter es más que trascendental para que la institución pueda garantizar que sus datos están a salvo y sin riesgo de ser vendidos o utilizados de forma indebida. El respeto a la confidencialidad no solo es una obligación legal, sino también un deber ético para aquellos que acceden y gestionan datos sensibles

2.1.12 De la recogida de datos sensibles

Los datos que se define como sensibles solo serán recogidos con el consentimiento expreso, teniendo la obligación quien recopila esta información de comunicarle el derecho que tienen para consentirlo o no y por consecuencia no entregar sus datos, salvo los casos en que la ley disponga que por interés general sean recabados, tratados y cedidos.

Este consentimiento tiene un origen distinto ya que "será una ley que prevea el tratamiento sin necesidad del consentimiento por parte del interesado, pues, el interés general suple la necesidad del mismo" (Rebollo Delgado & Mercedes Serrano, 2008). Esta necesidad no puede ser una violación manifiesta del derecho a la protección de datos debido a que el espíritu legislativo siempre será el bien común, teniendo como prioridad el bienestar del afectado, por ejemplo, los datos relativos a la salud.

Existe una excepción a la posibilidad de negarse al entregar los datos sensibles y esta radica en casuísticas específicas, siempre que el fin del uso de eso datos sensibles responda a la razón de existir de la entidad a la que se quiere pertenecer, los datos que se encuentren en el fichero de un partido político al que se pertenece, los relativos a la religión de la base de datos de la religión a la que pertenecieres, estos son algunos de los ejemplos que no se tiene el derecho a pertenecer a la entidad sin entregar sus datos sensibles, no obstante siempre debe existir previamente el consentimiento para la cesión de datos.

2.1.13 El consentimiento en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos

Con el avasallante desarrollo del comercio electrónico a nivel mundial a inicios de los dos mil, la sociedad ecuatoriana prevé que es necesario regularlo, porque el clásico comercio se encuentra en metamorfosis debido a que le medio donde se realiza el intercambio de bienes y servicios ahora se realiza a través de contratos electrónicos y su masificación se acompaña del desarrollo del internet. Con este desarrollo se presentan nuevas propuestas de contratos que se orientan a una perspectiva distinta de elementos como la no negociación, dando como origen a los contratos de adhesión, donde lo único que se solicita es el consentimiento de las partes al firmar el mismo.

Sobre este consentimiento la Ley de comercio electrónico, firmas electrónicas y mensaje de datos establece dos distinciones, la primera versa sobre el consentimiento para aceptar mensajes de datos, que define cuales son los elementos para consentir el uso de mensajes de datos y el registro electrónico, el primer elemento de este consentimiento es la información, la cual de ser "clara, precisa y satisfactoria" (Ley de Comercio Electrónico, firmas y mensajes de datos) Art 48 y el segundo elemento es el acceso a la información que va a ceder objeto de ese consentimiento.

El segundo tipo de consentimiento es el que se da para el uso de medios electrónicos, la característica de este consentimiento se presenta a través de una disposición donde se requiere que toda la información en relación al servicio relacionado al comercio electrónico deba constar por escrito a través de los medios electrónicos, con esto se busca que el consentimiento sea informado, este consentimiento se define como "el acuerdo o concurso de voluntades que tiene por objeto la creación o transmisión de derechos y obligaciones que puede ser en el campo de una relación de consumo" (Montalvo, 2007, pág. 71). Para que esta transmisión de derechos se perfeccione el consumidor debió expresamente autorizar el consentimiento y previamente a otorgarlo se le debió informar de forma clara y precisa sobre sus derechos a la posibilidad de recibir la información por escrito o medios electrónicos, a cancelar el consentimiento bajo las respectivas sanaciones de hacerlo posteriormente, cuáles son los procedimientos para retirar el consentimiento y para poder recibir la información impresa

2.1.14 El responsable del tratamiento

La persona que tiene a cargo la responsabilidad del tratamiento de los datos personales y sensibles de un usuario/titular, es decir el que debe determinar cuál es la finalidad de la recolección de este tipo de información, tiene en sus hombros la obligación de dar como garantía al sujeto que está siendo objeto del procesamiento de datos en todo momento la certeza de la conservación de sus derechos, tales como se ha mencionado anteriormente, la intimidad, privacidad, autonomía, dignidad humana, etc.

Según lo manifestado por el autor Vergara Rojas, Manuel (2017):

> es conveniente que se establezca de forma más clara y definida la exigencia, especialmente en el caso de las personas jurídicas que traten datos, de designar a un encargado del tratamiento de datos que sea persona natural, sea que actúe solo o al mando de otras personas. Asimismo, si la entidad encomienda a otras el tratamiento de datos debe establecerse la obligación de que la empresa encargada designe o tenga en su estructura a un encargado del tratamiento de datos. Todo esto para efectos de responsabilidad y eventuales reclamos. (Vergara Rojas, Manuel, 2017, pág. 146)

De acuerdo con Manuel Vergara en la Revista chilena de derecho y tecnología en su apartado Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales, ya que establece el por qué tiene mucha relevancia determinar quién es el individuo responsable de manejar

esta información dentro de una entidad, independientemente si esta es pública o privada, debido a que ellos se van a encargar del tratamiento de datos sensibles, debe tener claras sus limitaciones y objetivos con dicha información, aun cuando estas instituciones contraten o se vean en la necesidad de delegar a un encargado que esté bajo la orden de otro, todos deben conocer sus responsabilidades y hacer frente cuando un usuario busque realizar una queja referente a la divulgación de sus datos. De este modo, el titular puede asegurarse de que hay una persona que se pueda identificar en caso de resultar una situación legal o reclamo con ella.

Considerando que para que todo esto sea posible no es cuestión de solo simplemente confiar en que los encargados del tratamiento no cambiaran la finalidad de la recolección de datos para hacer un uso indebido y con fines distintos a los que estaban destinados, sino de que exista una implementación de regulaciones que ayuden a establecer un adecuado cuidado para de esta manera proteger los derechos e intereses de los titulares de la información recolectada, no solamente en los organismos públicos, también en los privados, en especial en aquellos que se manejan a través de la web y que están casi exentos de culpa, ya que es muy difícil determinar quién divulgó algo en internet.

En cuanto las entidades como plataformas en línea y que su funcionamiento es exclusivamente a través de un entorno virtual, es posible decir que implica un riesgo mayor que al manejo manual de datos, debido a que tienden a tener una mayor recopilación de información de usuarios, desde nombres y correos, hasta detalles que requieren de mucha más sensibilidad como preferencias sexuales, por ello necesitan estar mejor preparados en ciberseguridad para poder resguardar la información recolectada contra ciberataques; es decir, un mejor protocolo de seguridad en caso de fugas de datos, politicas mucho más detalladas y que se puedan entender de manera sencillas y claras.

En síntesis, la persona encargada del tratamiento de datos tiene una responsabilidad fundamental: garantizar que los derechos del titular de los datos, como la privacidad, la autonomía y la dignidad, se conserven en todo momento, por ello es importante definir claramente quién asume este papel, ya sea en empresas que manejan datos o en aquellas que los subcontratan. Esta designación establece responsabilidades claras para proteger los datos y enfrentar posibles reclamos o situaciones legales.

Sin embargo, confiar únicamente en la buena fe de los encargados del tratamiento no es suficiente, se necesitan regulaciones sólidas que establezcan pautas claras para proteger los derechos e intereses de los titulares de los datos, especialmente en el ámbito digital, donde la identificación de los responsables puede ser más compleja y donde la divulgación indebida de información es más difícil de rastrear.

2.1.15 Habeas Data

Origen

Visto desde la etimología el habeas data proviene del latín -hábeas- que significa conservar o guardar y -data- cuyo significado es dato, entonces su definición es -guardar el dato-, esto es custodiar la información otorgada por los individuos.

Sus inicios desde la perspectiva histórica se dan en Estados unidos con la -Privacity Act- en 1974, y tenía por objetivo la regulación de la protección de la privacidad en los ciudadanos estadounidenses y brindarles el control sobre su información personal almacenadas por agencias gubernamentales; En América del sur se dieron poco a poco en sus leyes iniciando por Brasil en 1988, Colombia en 1991, Paraguay en 1992, continuando por Perú en 1993, Argentina 1994 y Venezuela en 1999. Por otro lado en Centro América siendo mencionado en disposiciones específicas en Guatemala en 1985, Nicaragua en su constitución de 1987.

En Ecuador, apareció por primera vez en la Constitución Política de 1996, garantizando el acceso y conocimiento de información personal en poder de entidades públicas o privadas, con derecho a actualización, rectificación o eliminación si fuese errónea o afectase derechos, continuada por la Ley de Control Constitucional de 1997 la cual definió el Hábeas Data, permitiendo a personas naturales o jurídicas acceder a datos personales y exigir respuestas y medidas protectoras. Posteriormente, en 1998, la Carta Magna incorporó el Hábeas Data, respaldando a los individuos el acceso a documentos, bancos de datos e informes, con derecho a actualización, rectificación o eliminación en caso de que se vieran afectados sus derechos y finalmente, la Constitución del 28 de septiembre de 2008 que reafirmó estos derechos, asegurando el acceso a documentos, datos personales y archivos, con la posibilidad de solicitar su actualización, rectificación o eliminación, con medidas de seguridad para datos sensibles y la opción de demandar por perjuicios causados si no se atienden las solicitudes.

La acción

El habeas data puede ser considerado la piedra angular en la protección de derechos como la privacidad, da la garantía a las personas del control de sus datos, resguardando su uso por parte de terceras personas/entidades; es decir, busca propiciar la autodeterminación informativa, dando a cada individuo el poder de decidir cómo se utilizan sus datos, evitando posibles abusos de información por instituciones que obtienen beneficios a expensas de la privacidad. Además de leyes y regulaciones, se debe tener mecanismos de protección, ya que no lo es un impacto para el área legal, sino que también afecta la confianza y la ética en la sociedad. Esta acción tiene una gran importancia ya que da la posibilidad de intervenir en caso de que los datos que se tienen sobre las personas no son correctos o si estos están siendo utilizados de manera inapropiada, ofreciendo al sujeto de esta manera la libertad de decidir quién puede acceder a la información y con qué propósito, concediendo una especie de voz en cómo se gestiona y utiliza la identidad digital.

Con las nuevas tecnologías y el uso de redes, la información fluye a velocidades inimaginables, yendo de una frontera a otra en cuestión de segundos, por lo que el control de la información personal no es algo que se pueda tener en su totalidad En resumidas cuentas, la evolución del habeas data de sus raíces etimológicas hasta su expansión por distintos países de América Latina evidencia su importancia como pilar fundamental en la protección de la privacidad y la autodeterminación informativa. Este principio, derivado del latín y que significa literalmente "guardar el dato", ha sido clave en la garantía del control que las personas tienen sobre su propia información. Desde su surgimiento en Estados Unidos con la Privacy Act en 1974 hasta su inclusión en las constituciones y leyes de países sudamericanos, así como en Centroamérica, el habeas data ha sido un factor significativo para otorgar a los individuos el derecho de acceder, rectificar y controlar la información que otros poseen sobre ellos. En el contexto ecuatoriano, esta acción constitucional se ha fortalecido, otorgando a los ciudadanos la facultad de intervenir y corregir datos incorrectos, así como de solicitar la eliminación de información inapropiada; además, la posibilidad de exigir medidas de seguridad para datos sensibles y la opción de demandar por perjuicios ocasionados ofrece una protección adicional. El habeas data, al garantizar la intervención y el control sobre la información personal, ofrece una especie de voz a los individuos en la gestión de su identidad digital, permitiéndoles intervenir y proteger sus datos, asegurando un equilibrio entre la innovación tecnológica y la protección de los derechos individuales.

2.2 Marco Legal

CONSTITUCIÓN DEL ECUADOR

Entre los antecedentes más relevantes de la protección de datos y la privacidad en Ecuador está la constitución de 2008, debido a que es un tema relativamente nuevo y que van en evolución, ya que si bien la constitución de 1998 no contenía disposiciones específicas sobre protección de datos o intimidad en el sentido contemporáneo, sentó las bases para el reconocimiento de derechos fundamentales y estableció el principio de que el Estado debe proteger y garantizar los derechos humanos.

Uno de los derechos inherentes de las personas es el de libertad, que se toma como un cimiento para la autonomía del individuo, que podría explicarse como la propia construcción del ser, como la capacidad de actuar y de tomar decisiones, que son solo la cúspide de muchas más libertades como de expresión, asociación, religiosa o de movimiento. Naturalmente es una obligación del estado mantener a sus ciudadanos con la seguridad de que estos no se verán vulnerados.

Bajo este contexto los legisladores ecuatorianos enmarcan en la constitución de la república del ecuador una serie de derechos fundamentales para sus ciudadanos, como el art 66 y sus numerales, donde menciona que se reconoce y garantizará a las personas:

> 11. El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica.

El numeral del artículo referido aborda puntos importantes, principalmente sobre la importancia de la conservación de las convicciones que podría entenderse como una idea propia de un determinado individuo, por lo que este, respetando su independencia, no puede ser obligado a revelar información sobre sus creencias religiosas, filiación política u opiniones personales. Otro de los puntos esenciales dentro del enumerado es que prohíbe especialmente la exigencia o uso de datos personales sin la autorización del titular, más aún si la información de la que se habla es parte de los datos sensibles de un individuo como aquellos relativos a: etnia, identidad de género, pasado judicial, datos biométricos, entre otros; porque la divulgación de estos últimos, pueden traer como consecuencias considerables para la persona afectada. Y finalmente, las excepciones que se establecen para

necesidades de atención médica, esto indica que, en situaciones en las que la divulgación de información sobre la salud sea necesaria para brindar atención médica adecuada, se permite el acceso a estos datos. Sin embargo, esto debe hacerse respetando la confidencialidad y privacidad del paciente, y solo debe revelarse la información necesaria para el tratamiento médico.

> 19. as derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Este derecho reconoce la importancia de proteger la información personal de los individuos, compromete que cada persona tiene el derecho fundamental a que sus datos personales sean tratados de manera adecuada, segura y respetuosa con su privacidad, además de tener acceso a información que haya sido recopilada sobre estas y decisión sobre su manejo y requiriendo su autorización para su recolección, almacenamiento, procesamiento, distribución o difusión, de esta manera se procura la legitimidad de su privacidad.

El mencionado principio de consentimiento informado (el que parte de las empresas hacia sus usuarios) resulta fundamental para proteger la privacidad y autonomía de las personas, de esta manera se puede decir que se garantiza el que las personas tengan control sobre su información

> "20. El derecho a la intimidad personal y familiar".

El gobierno debe garantizar la seguridad de sus ciudadanos, protegiendo su derecho a la privacidad tanto individual como familiar. Esto significa que cada persona tiene el derecho de mantener secretos aspectos importantes de su vida, como su hogar, sus conversaciones personales y su rutina diaria, sin que nadie, incluso el gobierno, interfiera sin permiso. Además, las familias también tienen derecho a mantener su vida privada dentro de su propio círculo, protegiendo sus relaciones y comunicaciones de intrusiones no deseadas. Esto implica que nadie debería obtener información personal sin autorización, como leer correos electrónicos privados o hacer vigilancia sin motivo. Todo esto se hace en respeto a la dignidad de cada individuo y su familia, reconociendo que todos merecen ser tratados con respeto y tener su espacio personal protegido.

> "25. EI derecho a acceder a bienes y servicios públicos y privados de calidad, con eficiencia, eficacia y buen trato, así como a recibir información adecuada y veraz sobre su contenido y características."

Este numeral, del artículo 66 de la Constitución asegura que las personas tienen derecho a acceder a una amplia variedad de bienes y servicios, tanto públicos como privados, que cumplan con estándares de calidad. Esto significa que deben recibir un trato eficiente, amable y respetuoso al utilizar estos servicios. Además, es fundamental que tengan acceso a información clara y precisa sobre los mismos, garantizando que sea veraz y completa para que puedan tomar decisiones informadas. Este derecho promueve la libertad, autonomía e intimidad personal al permitir que cada individuo elija los servicios que desea sin temor a engaños o información sesgada

LA DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS

La Declaración Universal de Derechos Humanos (DUDH) nace en 1948 a partir de tres tipos de conflictos suscitados entre los individuos, tales como conflictos sociales cuya demanda son por colectivos vulnerables y movimientos sociales hacia grupos privilegiados; los conflictos políticos que legitimaban los abusos a la dignidad de los sujetos, y por último los conflictos internacionales que surgen a partir de comportamientos crueles para excusar ideales distintos al bien común, se crea como una reacción a los horrores de la Segunda Guerra Mundial en 1945, la premisa de la existencia de un marco común para garantizar los derechos humanos, cuya necesidad se basaba la protección de los individuos, la creación de un nuevo orden mundial con la fundación de la ONU para la promoción y salvaguarda de estos derechos, el trabajo de los principales defensores y la consolidación de las normas existentes, ya que no se creó nuevos derechos, sino que se consolidó y codificó principios que ya existían en diversas tradiciones legales, filosóficas y religiosas de todo el mundo en un documento que tenía un alcance global, de esta manera emerge una base en que los estados podrían establecerse para la construcción de sus propios sistemas de protección de derechos . dichos principios universales ayudarían a regir las relaciones entre los Estados y garantizar los derechos inherentes de todas las personas, la DUDH dio paso para que se realizara la firma de dos convenios igual de importantes como el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales.

La declaración reconoce a la libertad como parte de la dignidad, de la misma manera que la igualdad entre todos los hombres, por lo que nadie tiene -derecho- de vulnerar a otro, entonces las naciones deben cuidado de injerencias y ataques a los individuos como está establecido en el art 12 de la declaración:

> Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

El artículo 12 de la Declaración Universal de Derechos Humanos indica que cada individuo tiene derecho a delimitar lo que puede y no saberse de sí mismo, es decir, a marcar una diferencia entre lo que comúnmente se llama vida privada y vida pública. Este artículo reconoce el derecho fundamental a la privacidad y protege a las personas contra cualquier interferencia injustificada en aspectos íntimos de sus vidas, como sus relaciones personales, la seguridad de su hogar y la confidencialidad de sus comunicaciones. Además, resalta la importancia de la protección legal para garantizar estos derechos, permitiendo a las personas buscar soluciones legales en caso de violación de su privacidad o ataques a su reputación. En conclusión, busca salvaguardar la dignidad y la autonomía de los individuos al garantizar su derecho a mantener ciertos aspectos de sus vidas fuera del escrutinio público y protegerlos contra cualquier interferencia injustificada por parte de autoridades u otros actores.

PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS

El Pacto Internacional De Derechos Civiles Y Políticos adoptado por la Asamblea General de las Naciones Unidas el 16 de diciembre de 1966, data su origen junto a la declaración universal de los derechos humanos de 1948, que estableció principios valiosos para el amparo de los derechos y se reconoció la necesidad de fijar tratados vinculantes que le dieran a una fuerza legal más sólida a la DUDH.

Entre ellos está el PIDCP que entró en vigor en 1976, después de que un número suficiente de países lo ratificara, desde entonces tuvo gran acogida y un impacto significativo a nivel internacional, siendo usado como referencia en casos judiciales y como piedra angular para el desarrollo de leyes nacionales.

Estableció un conjunto de derechos civiles y políticos fundamentales, como el derecho a la vida, la libertad de expresión, la libertad de religión, el derecho a un juicio justo y el derecho a la privacidad como indica el art 17 y 19.

> “Artículo 17.1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.”
>
> “Artículo 17.2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.”

El art 17.1 prohíbe cualquier tipo de intervención o acción en la vida privada, la familia, el domicilio o la correspondencia de una persona que sea injustificada, ilegal o sin autorización legal. Incluyendo acciones como la vigilancia sin consentimiento, los allanamientos sin una orden judicial válida, la interceptación de comunicaciones privadas, entre otras, también protege contra ataques ilegales a la honra y la reputación de una persona, como la calumnia.

Mientras que el 17.2 fundamenta que toda persona tiene derecho a buscar recursos legales en caso de que sus derechos sean vulnerados o se vean afectados por ataques a su dignidad y reputación. Esto garantiza que de cierta manera existan mecanismos legales efectivos para proteger estos derechos y responsabilizar a quienes los vulneren.

> Artículo 19.1. Nadie podrá ser molestado a causa de sus opiniones.
>
> Artículo 19.2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
>
> Artículo 19.3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:
>
> a) Asegurar el respeto a los derechos o a la reputación de los demás;
>
> b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas.

En conformidad con este artículo, los individuos son libres de expresar opiniones y no ser juzgados a causa de esto, incluyendo que no puede ser molestados o perseguidos, es decir, sin sufrir represalias o censura por parte de autoridades gubernamentales, grupos políticos, etc., dicha libertad comprende buscar, recibir y difundir información referente a cualquier tema que este considera importante además de utilizar algún medio que se requiera para difundir sus ideales. Se debe guardar responsabilidad e ir acorde a la ley, sin ningún tipo de discriminación a cualquier persona, evitando que se llegue a la difamación, la calumnia o el discurso de odio que pueda causar daño a otros y generar violencia, para poder mantener el orden público

LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

La ley orgánica de protección de datos personales se origina a partir de una filtración masiva de datos en 2019 y una posible violación a la privacidad que fue descubierta por Noam Rotem y Ran Lokar, expertos informáticos de vpnMentor, que comprenden información sensible como su posición financiera hasta datos familiares, situación peligrosa ya que estaban expuestos a varios delios como ciberataques, estafas, robo de dinero, etc.

Fue presentada como un proyecto de ley por el presidente de ese año Lenin Moreno, reconociendo la importancia de proteger los datos personales de los ciudadanos ecuatorianos en un entorno cada vez más digitalizado.
Dentro de este cuerpo normativo se existen figuras como el consentimiento que permite a la persona acceder o negarse a dar s información, también se establecen principios con los que se rige y en qué circunstancias podría darse el tratamiento de la información.

> **Art. 8.- Consentimiento. -** Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea:
>
> 1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento;
>
> 2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento;
>
> 3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia,
>
> 4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular.
>
> El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento.
>
> El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos.
>
> Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste que dicho consentimiento se otorga para todas ellas.

El consentimiento es la manifestación de la voluntad, y esta tiene características propias para poder tratarse y comunicarse datos personales, como ser libre de los vicios del consentimiento que son error, fuerza y dolo, lo que significa que debe ser dado sin coerción, amenaza, fraude o cualquier otro tipo de influencia indebida, sin ningún tipo de presión

externa; debe ser especifica, esto es que el titular de los datos debe estar informado claramente sobre los propósitos para los cuales se utilizarán sus datos personales, estableciendo los puntos claros sobre el medio y el fin del tratamiento; debe ser informado, o sea que el titular debe recibir la información clara y completa sobre el uso de sus datos, garantizando a transparencia en el procesamiento de datos y permite que el titular tome decisiones informadas sobre el tratamiento de sus datos; debe ser inequívoco, no debe haber dudas sobre el alcance de la autorización otorgada por el titular de los dato

> Art. 10.- Principios. - Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de
>
> b) Lealtad. - El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados.
>
> En ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales.
>
> c) Transparencia. - El tratamiento de datos personales deberá ser transparente, por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro.
>
> Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia.
>
> d) Finalidad. - Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular: no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta Ley.
>
> El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

Los principios que rigen este cuerpo normativo tienen como objeto garantizar la privacidad de las personas y promover la confianza en el manejo de la información personal de los

individuos, buscan asegurar el cumplimiento de la normativa en materia de protección de datos, proteger los derechos individuales y prevenir el uso indebido de la información personal.

Bajo esta premisa, el principio de lealtad se da porque la recolección, uso y manejo de datos debe darse de la manera más clara y honesta posible, las personas deben saber qué datos se están recopilando sobre ellas y cómo se utilizarán, añadiendo que, está prohibido tratar los datos de manera ilegal o deshonesta; el principio de transparencia determina que toda la información relacionada con el tratamiento de datos personales debe ser fácilmente accesible y comprensible para las personas, por tanto la comunicación debe ser clara y lo más sencilla posible; y el principio de finalidad porque es importante que se establezcan claramente los propósitos para los cuales se van a utilizar los datos personales, estos deben ser específicos, legítimos y comunicados al titular de los datos, no se pueden usar los datos para fines diferentes a los que se recopilaron inicialmente, a menos que exista una razón válida y legal para hacerlo. Adicionando que cualquier uso nuevo de los datos debe ser compatible con el propósito original y tener en cuenta las expectativas razonables de la persona sobre cómo se utilizará su información.

> **Art. 26.- Tratamiento de datos sensibles. -** Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias:
>
> a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines.
>
> b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social.
>
> c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento.
>
> d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos.
>
> e) El tratamiento se lo realiza por orden de autoridad judicial.
>
> f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.

g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente Ley.

En este artículo se menciona que solo es posible el tratamiento de datos personales de carácter sensible en ciertas circunstancias como teniendo el consentimiento explícito del titular, determinando clara mente los fines para los que será utilizado este tipo de información, por lo que el sujeto del tratamiento debe estar plenamente informado y consiente de. Uso que le darán a los datos sensibles; se puede dar el procedimiento en casos en que lo requiera para poder cumplir obligaciones legales o por situaciones laborales y seguridad social, para realizar evaluaciones médicas por ejemplo; se autoriza el tratamiento de datos sensibles cuando es necesario para proteger los intereses vitales del titular o de otra persona, en casos donde el titular no pueda dar su consentimiento debido a incapacidad física o legal, ocasiones en la que la salud o la vida de la persona esté en peligro; si los datos sensibles han sido voluntariamente divulgados por el titular, su tratamiento está permitido; puede darse por orden judicial como situaciones en las que la autoridad judicial considera que el tratamiento de datos es necesario para el cumplimiento de la ley o para el desarrollo de un proceso judicial; se permite el tratamiento de datos sensibles con fines de interés público, investigación científica o histórica, y estadísticas, siempre y cuando se respeten los derechos de privacidad del titular y se establezcan medidas adecuadas para proteger sus intereses y derechos; se autoriza cuando la vida o salud de una persona esté en riesgo como se ha mencionado anteriormente, es decir, solo se debe revelar la información estrictamente necesaria para el tratamiento médico.

REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

El 26 de mayo de 2021 fue expedido el reglamento de la ley orgánica de protección de datos personales, con la finalidad de elaborar las reglas necesarias para implementar esta ley y garantizar la salvaguarda de los derechos y libertades esenciales de las personas cuyos datos personales se ven afectados. Este reglamento proporciona las especificaciones y los procedimientos que no se abordan en la ley, incrementando la transparencia y la responsabilidad en la aplicación de la legislación, al detallar los procedimientos que permiten a ciudadanos y empresas entender claramente lo que se espera de ellos, y establecen componentes de supervisión que aseguran el cumplimiento de las normas.

> Art. 5.- De la recogida del consentimiento. - El responsable de datos personales deberá obtener el consentimiento del titular de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales.
>
> En todos los casos en los que de conformidad con la Ley se requiera el consentimiento explícito del titular para el tratamiento de sus datos, el responsable deberá informar previa y detalladamente los tipos de tratamiento, finalidades, el tiempo de conservación, las medidas de protección a adoptarse, las consecuencias de su entrega, entre otros aspectos determinados en la Ley, lo cual deberá ser consentido inequívocamente por el titular.
>
> El consentimiento del titular deberá reflejar de manera indubitada la aceptación de éste en relación con el tratamiento de sus datos personales a través de una declaración, pronunciamiento para darse de baja o clara acción afirmativa. El consentimiento otorgado por el titular deberá ser demostrado por el responsable que lo obtiene, cuando así sea requerido por la autoridad competente.
>
> Cuando los datos personales recogidos pertenecen a un incapaz, bastará con el consentimiento del representante legal debidamente acreditado ante el responsable, en los términos señalados en el presente artículo. El consentimiento de niñas, niños y adolescentes y, en general, de personas incapaces, se obtendrá a través de sus representantes legales y curadores, según lo dispuesto en la Ley Orgánica de Protección de Datos Personales y el Código Civil.
>
> El silencio o la inacción, por sí solos, no presumen el consentimiento del titular.

El Artículo 5 del RLOPDP establece las disposiciones que deben seguir los responsables de datos personales para obtener el consentimiento del titular, es imperativo que el consentimiento sea explícito cuando así lo requiera la normativa, esto involucra que el responsable debe proporcionar información detallada y previa sobre los tipos de tratamiento a los que se someterán los datos, las finalidades de dicho tratamiento, el tiempo de conservación de los datos, las medidas de protección que se adoptarán, y las consecuencias de la entrega de estos datos. Esta información debe ser presentada de tal forma que el titular pueda dar su consentimiento de manera inequívoca.

El consentimiento debe manifestarse de manera clara y no puede asumirse por silencio o inacción, es decir, debe reflejarse a través de una declaración explícita, una acción afirmativa clara, o una solicitud de baja. Además, el responsable de los datos debe poder demostrar que ha obtenido dicho consentimiento si alguna autoridad competente así lo requiere.

En los casos donde los datos personales pertenezcan a personas incapaces, como menores de edad, el consentimiento debe ser otorgado por sus representantes legales debidamente acreditados, esto supone a los tutores y curadores, según lo dispuesto en la Ley

Subraya la importancia de la sinceridad y la nitidez en el proceso de obtención del consentimiento, protegiendo así los derechos del titular de los datos, al exigir un consentimiento explícito e inequívoco, la ley busca evitar cualquier tipo de ambigüedad o malentendido, asegurando que los titulares estén plenamente informados y conscientes de cómo y para qué se utilizarán sus datos personales. Esto no solo protege a los titulares, sino que también obliga a los responsables a adoptar prácticas rigurosas y éticas en el manejo de la información personal, promoviendo una mayor responsabilidad y transparencia en el tratamiento de datos personales.

> Art. 6.- De la revocatoria del consentimiento. - El titular tendrá derecho a retirar su consentimiento en cualquier momento. La revocatoria del consentimiento no afectará a la licitud del tratamiento de datos llevado a cabo hasta el momento de la revocatoria. El responsable del tratamiento deberá contar con un procedimiento sencillo para que el titular pueda revocar su consentimiento.
>
> El responsable del tratamiento deberá suspender el tratamiento de los datos del titular que haya revocado su consentimiento, una vez recibida la notificación por parte del titular.

Este artículo versa sobre el derecho de una persona que puede retirar su consentimiento para el uso de sus datos personales o sensibles en cualquier momento, esto significaría que pueda cambiar de opinión o revocar el permiso que ha dado cuando lo desee, destacando que esto no necesariamente sea por el uso ilegal de su información, en otras palabras todo tratamiento de datos que se llevó a cabo con el consentimiento válido en su momento sigue siendo legal incluso después de la revocación, para esto el reglamento expone un procedimiento fácil de seguir y accesible para que cualquier persona pueda retirar su consentimiento sin impedimento alguno de esta manera garantizando que el proceso sea práctico y fácil.

Esto es que una vez que el responsable del tratamiento recibe la notificación de que la persona ha retirado su consentimiento debes estar inmediatamente cualquier tratamiento de los datos de esa persona incluyendo detener el uso activo de los datos y seguridad que no se procesen compartan o utilicen en el futuro

LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS

La ley de comercio electrónico firmas electrónicas y mensajes de datos expedida el 17 de abril de 2002 durante el mandato del abogado Gustavo José Joaquín Novoa bejarano cuyo período fue desde el 2000 al 2003, con el propósito de otorgar y reconocer la validez y el efecto jurídico que tienen las firmas electrónicas los mensajes de datos y toda información

que sea en formato digital indistintamente de su soporte físico y que se pueda atribuir a personas naturales o jurídicas tanto públicas como privadas

Este cuerpo legal establece normas relacionadas con el uso del internet debido a su importancia en el desarrollo del comercio tanto a nivel nacional como internacional, abarcando tanto el sector privado como el público con la finalidad de facilitar el acceso a los servicios electrónicos, permitiendo regular y controlar la utilización de estos sistemas, en el contexto del consentimiento para el uso de datos personales y a través de medios electrónicos esta ley asegura que la autorización otorgada por los individuos para el manejo de sus datos sea válida y jurídicamente efectiva independientemente del formato.

> Art. 49.- Consentimiento para el uso de medios electrónicos. - De requerirse que la información relativa a un servicio electrónico, incluido el comercio electrónico, deba constar por escrito, el uso de medios electrónicos para proporcionar o permitir el acceso a esa información, será válido si:
>
> a) El consumidor ha consentido expresamente en tal uso y no ha objetado tal consentimiento; y,
>
> b) El consumidor en forma previa a su consentimiento ha sido informado, a satisfacción, de forma clara y precisa, sobre:
>
> 1. Su derecho u opción de recibir la información en papel o por medios no electrónicos;
>
> 2. Su derecho a objetar su consentimiento en lo posterior y las consecuencias de cualquier tipo al hacerlo, incluidas la terminación contractual o el pago de cualquier tarifa por dicha acción;
>
> 3. Los procedimientos a seguir por parte del consumidor para retirar su consentimiento y para actualizar la información proporcionada; y,
>
> 4. Los procedimientos para que, posteriormente al consentimiento, el consumidor pueda obtener una copia impresa en papel de los registros electrónicos y el costo de esta copia, en caso de existir.

El artículo 49 de la ley de comercio electrónico firmas electrónicas y mensajes de datos establece disposiciones sobre el consentimiento que es necesario para el uso de medios electrónicos en la suministro de la información que se relaciona con los servicios digitales, incluyendo el comercio electrónico, describe el consentimiento como expreso y subraya la importancia y necesidad de que el consumidor manifieste expresamente su consentimiento para el uso de medios electrónicos que debe ser claro y no objetado posteriormente por este, de esta manera se garantiza que el consumidor esté consciente y de acuerdo con el uso de estos medios reforzando así el principio de autonomía contractual y protegiendo sus derechos

como consumidor. Para que este consentimiento se valide el consumidor debe estar completamente informado sobre todo los aspectos antes de dar su autorización implicando que esta información debe ser comprensible y accesible para que se pueda tomar una decisión informada, debe incluirse que si desea recibir esta comunicación de manera directa y no a través de un medio digital para así asegurar que la persona no esté obligado a aceptar medios electrónicos si prefiere los formatos tradicionales, también se debe poner a conocimiento que puede retirar su consentimiento en un futuro y en caso de que haya alguna consecuencia como el pago de tarifas adicionales se, le debe decir, y que la persona prevea la posible relación contractual.

2.3 Marco Conceptual

Consentimiento: La acción y resultado de consentir proviene del latín "consentire", compuesto por "cum" (con) y "sentire" (sentir), lo que implica compartir un sentimiento o parecer. Consiste en permitir algo o acceder a que se lleve a cabo. Es la expresión de una voluntad coincidente entre la oferta y la aceptación, y constituye uno de los requisitos fundamentales que los códigos legales exigen para la formación de contratos.

Dato sensible: Referido a información que requiere una protección especial, también conocido como dato especialmente protegido.

Datos sensibles: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales. (Ley Orgánica de Protección de Datos Personales)

Responsable de tratamiento de datos personales: persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales. (Ley Orgánica de Protección de Datos Personales)

Revocar: anular una manifestación de voluntad o un acto legal en el que una parte tiene la facultad unilateral de hacerlo, como por ejemplo un testamento, un mandato o una donación (en determinadas circunstancias), entre otros.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales. (Ley Orgánica de Protección de Datos Personales)

CAPÍTULO III:

3. MARCO METODOLÓGICO

3.1 Diseño de investigación

En la presente investigación se realizó el estudio del Consentimiento en el uso de datos sensibles y la Ley Orgánica de Protección de Datos en el ámbito privado, 2023 y se desarrolló considerando el enfoque cualitativo debido a que se describió el fenómeno de forma deductiva desde la comprensión del derecho a la protección de datos como una garantía a la protección de los derechos establecidos en la declaración de los Derechos humanos y en nuestra Constitución de la República del Ecuador hasta de forma específica la comprensión de los elementos del consentimiento para que el tratamiento que se les dé sea legal y legítimo, se utilizó una muestra pequeña no probabilista para identificar si se conoce el alcance que se le otorga a la entidad encargada del tratamiento de datos sensibles, además se busca plantear nuevas hipótesis sobre el derecho humano a la protección de datos y así descubrir nuevos conocimientos. (REYES, BRENDA; CASTILLO, CARLOS, 2015)

Tipo de investigación

Según establece la taxonomía de la investigación desarrollada en la obra (GUIA METODOLOGICA PARA PROYECTOS DE INVESTIGACIÓN SOCIAL) esta investigación según el nivel de conocimiento se realizó usando el tipo exploratorio, ya que se averiguó qué está pasando con el objeto de estudio a través de información documental, entrevistas y encuestas que permitan conocer el fenómeno a estudiar que previamente ha sido desconocido y resolver algunas interrogantes que giren en torno a nuestra hipótesis.

3.2 Recolección de la información

Para iniciar el proceso de investigación, es esencial establecer herramientas que faciliten la recolección y el análisis de datos. En este estudio, se ha decidido utilizar guías de Entrevistas y encuestas como medios para interactuar con los miembros de la muestra seleccionada. Estas herramientas están diseñadas para abordar las dos variables de investigación: el consentimiento para el uso de datos sensibles y la ley orgánica de protección de datos

personales en el ámbito privado. De esta manera, se garantiza una conexión efectiva con los participantes y se asegura que la investigación cumpla con las normativas legales vigentes.

Población

La población se refiere al grupo de elementos vinculados al objeto de estudio. Se trata de los componentes, cuya principal finalidad es recopilar información durante la investigación. Básicamente, la población incluye a todos los elementos, como individuos, organismos u objetos, que forman parte del fenómeno definido y delimitado en el análisis del problema de investigación, por ello, se ha considerado que la provincia de Santa Elena es la población idónea, ya que cumple con gran parte de estos elementos.

CUADRO 1: POBLACIÓN

ELEMENTOS	NI
Constitución de la República del Ecuador	1
Ley Orgánica de protección de datos personales	1
Reglamento de la ley Orgánica de la protección de datos personales	1
Ley de Comercio Electrónico, firmas y mensajes de datos	1
Declaración de los derechos humanos	1
Declaración de los derechos civiles	1
Jueces de primera instancia de la provincia de Santa Elena	23
Representante de la DINARP, entidad encargada de la protección de datos personales.	1
Entidades privadas	10
Ciudadanos de la provincia de Santa Elena	385.735
TOTAL	385.775

Elaborado por: Luz Borbor y Wilson Chaca

Muestra

Debido a la universalidad de la población, se utilizó una muestra no probabilística por conveniencia, que consiste determinar la muestra en relación con los intereses del objeto de estudio y la capacidad de obtener la información, ya que los requerimientos de utilizar toda la población del Ecuador incrementarían los costos de la investigación.

Entrevistar a jueces facultados para resolver habeas data, sería fundamental para obtener una perspectiva jurídica sólida sobre el tema del consentimiento para el uso de datos sensibles

por parte de empresas privadas, ya que tienen experiencia en la interpretación y aplicación de leyes relacionadas con la privacidad y los derechos constitucionales, lo que brinda una comprensión profunda de los principios legales en juego, y se puede obtener una visión clara de cómo se abordan las cuestiones de privacidad y consentimiento en el ámbito legal.

La entrevista a un funcionario de la dirección nacional de registros públicos radica en su perspectiva institucional que proporciona una comprensión honda del marco legal y las políticas gubernamentales relacionadas con la protección de datos sensibles. Además, su experiencia práctica en el manejo de registros públicos le permite ofrecer información detallada sobre los procedimientos y protocolos establecidos para garantizar la seguridad y privacidad de dichos datos. Asimismo, puede los desafíos específicos en la protección de datos sensibles en el contexto empresarial, basado en su conocimiento, el funcionario puede ofrecer recomendaciones y perspectivas para mejorar las políticas y prácticas relacionadas con el consentimiento del uso de datos sensibles por parte de empresas privadas.

Se pone a consideración la entrevista a 2 entidades privadas, debido a que proveería una perspectiva invaluable sobre cómo se manejan y utilizan los datos sensibles en la práctica, ya que conoce detalles de los procesos internos de recopilación, almacenamiento y uso de datos dentro de la industria, así como los procedimientos establecidos para obtener el consentimiento de los usuarios para utilizar sus datos sensibles, dándonos la posibilidad de analizar nuestras teorías en la práctica.

Se seleccionó como población la provincia de Santa Elena, debido a que, dentro de este se encuentran una amplia gama de grupos demográficos, se capturan distintas opiniones y enfoques sobre el tema, proporcionando así un panorama más completo y enriquecido para el análisis de las encuestas.

Y por último, pero no menos importante entrevistar a una ciudadana, que ha experimentado la utilización ilegítima de sus datos sensibles, su testimonio brinda una perspectiva real y personal sobre los impactos negativos que pueden surgir cuando los datos sensibles caen en manos equivocadas, ilustrando de manera vívida los riesgos y las consecuencias de la falta de protección de la privacidad de los datos, demostrando las deficiencias en los sistemas de seguridad y protección de datos tanto a nivel gubernamental como en el sector privado, destacando áreas que requieren mejoras urgentes.

CUADRO 2 MUESTRA

ELEMENTOS	MUESTRA
Constitución de la República del Ecuador	1
Constitución de la República del Ecuador	1
Ley Orgánica de protección de datos personales	1
Reglamento de la ley Orgánica de la protección de datos personales	1
Ley de Comercio Electrónico, firmas y mensajes de datos	1
Declaración de los derechos humanos	1
Declaración de los derechos civiles	1
Jueces de primera instancia de la provincia de Santa Elena	3
Representante de la DINARP, entidad encargada de la protección de datos personales.	1
Entidades privadas	2
Ciudadanos de la provincia de Santa Elena	400 1
TOTAL	414

Elaborado por: Luz Borbor y Wilson Chaca

Métodos, Técnicas e Instrumentos

Método de análisis histórico jurídico

En el presente trabajo investigativo se hizo uso del método de análisis histórico jurídico, dada su capacidad para proporcionar una comprensión profunda y contextualizada del derecho a lo largo del tiempo, ya que, al analizar la evolución histórica, se logra trazar el desarrollo de las leyes, desde sus orígenes hasta su estado actual, permitiendo de esta manera identificar su evolución en distintos contextos como: políticos, sociales y culturales. La técnica principal fue una -matriz de análisis comparativo histórico del derecho a la protección de datos- donde se estableció su desarrollo de modo que fue más comprensible realizar una inmersión más profunda en dicho análisis. Esto implicó revisar de forma exhaustiva fuentes históricas, y documentos relevantes sobre el tema en cuestión, como doctrinas que centran su objetivo en la protección de datos personales, de autores destacados como Rebollo Delgado.

En el contexto del análisis histórico jurídico, se pudo emplear una técnica que combina la investigación documental exhaustiva con el enfoque contextual. Inicialmente, se recopilaron fuentes primarias como leyes, jurisprudencia y documentos legislativos relevantes para el periodo en estudio. Posteriormente, se llevó a cabo un análisis crítico de estas fuentes,

identificando patrones, cambios y continuidades en la evolución del marco legal. Además, se integró una perspectiva contextual, examinando factores sociales, políticos y económicos que influyeron en la formulación y aplicación de las leyes. Este enfoque holístico permitiría al investigador comprender no solo la evolución normativa, sino también su impacto en la sociedad y el sistema jurídico en cuestión.

Una herramienta fundamental para ejecutar la técnica de análisis histórico jurídico es una -matriz de análisis comparativo histórico del derecho a la protección de datos- con información extraída de la investigación, que facilite el acceso a fuentes primarias y secundarias relevantes. Bases de datos jurídicas, archivos históricos digitales y bibliotecas especializadas en derecho pueden ser recursos valiosos. Herramientas de búsqueda avanzada y análisis de texto también son esenciales para examinar grandes conjuntos de documentos de manera eficiente. Además, programas de gestión bibliográfica pueden ayudar a organizar y citar las fuentes de manera sistemática. Así también identificar patrones y tendencias en el desarrollo normativo a lo largo del tiempo. En resumen, una combinación de recursos digitales y herramientas especializadas optimizó el proceso de investigación y análisis en dentro de una matriz para hacer más eficiente el trajo de tesis.

El método de análisis exegético jurídico

Aplicar el método de análisis exegético jurídico en este documento fue importante, debido a que al ser utilizado aportó una interpretación más detallada y precisa que fue respaldada en documentos tanto legales como doctrina, de manera que se convirtió en una herramienta necesaria para dilucidar la aplicación y relevancia de leyes en situaciones contemporáneas, basándose en la lógica y la razón, usando principalmente como técnica el estudio de documentación significativa, y el instrumento clave en este método son los documentos legales en sí mismos.

En el marco del método exegético jurídico, se emplea una aproximación meticulosa y detallada a la interpretación de textos legales. Esta técnica implica un análisis profundo de la normativa, centrándose en el significado y la intención del legislador al redactar las disposiciones legales. Donde el lector se sumergirá en la hermenéutica jurídica, examinando no solo el texto en sí, sino también su contexto histórico, social y cultural. La identificación de términos clave, el análisis gramatical y la consideración de precedentes jurisprudenciales relevantes son elementos esenciales en este enfoque. La meta es descifrar con precisión el

contenido normativo y determinar cómo se aplica a situaciones específicas, proporcionando así una interpretación fundamentada y coherente en el ámbito legal.

En el contexto del método exegético jurídico, el uso de mapas conceptuales se presenta como una herramienta clásica pero efectiva para visualizar y organizar las relaciones entre los elementos clave en la interpretación legal. Este -mapa conceptual de simplificación descriptiva - pueden representar términos jurídicos, conceptos y sus interconexiones de manera gráfica, facilitando la comprensión y memorización de las complejidades normativas. Al crear un -mapa conceptual de simplificación descriptiva-, el investigador puede destacar la jerarquía de normas, identificar relaciones causa-efecto y resaltar precedentes jurisprudenciales relevantes. Esta técnica proporciona una visión estructurada que no solo ayuda en la comprensión profunda de los textos legales, sino que también sirve como una herramienta pedagógica valiosa para comunicar de manera clara y coherente los resultados de la investigación -consentimiento en el uso de datos sensibles y la ley Orgánica protección de datos personales en el ámbito privado, 2023-.

El método de campo

Se reconoce al método de campo como el más idóneo para desarrollar la recopilación de información de forma directa y detallada, dentro de este método, se emplean técnicas de campo específicas, como la entrevista, que consiste en un diálogo planificado entre el investigador y los participantes. En el caso específico del presente estudio, se aplicó esta técnica a los jueces del cantón La Libertad y a funcionario de la Dinardap. El instrumento utilizado para llevar a cabo las entrevistas fue un guion de preguntas, diseñado para explorar aspectos clave relacionados con el objeto de estudio. Este enfoque permitió profundizar en temas específicos y obtener información relevante de manera sistemática y detallada.

Además de las entrevistas, se implementó una encuesta dirigida a la ciudadanía para complementar el proceso de recolección de datos. Esta encuesta, realizada mediante un cuestionario estructurado, tenía como objetivo principal evaluar el nivel de conocimiento y percepción de la población sobre el tema de estudio.

El uso combinado de entrevistas y encuestas proporcionó una visión completa y enriquecedora del objeto de estudio, permitiendo así realizar un diagnóstico preciso.

3.3 Tratamiento de la información.

Para llevar a cabo un tratamiento adecuado de la información recolectada, se utilizaron diversos elementos esenciales. En la primera fase, se realizó una investigación bibliográfica para establecer el enfoque teórico y legal, reforzando así la base doctrinaria que sustenta la argumentación del estudio.

Posteriormente, se emplearon guías de entrevista dirigidas a jueces, un representante de DINARP, y entidades privadas. En el caso de los jueces, las entrevistas se realizaron después de cada audiencia para no interferir con su horario laboral. Lamentablemente, la entrevista programada con el representante de DINARP no pudo llevarse a cabo debido a la falta de respuesta y la premura del tiempo para la entrega del trabajo. Las entrevistas con las entidades privadas se realizaron vía Zoom fuera del horario laboral, ya que no era posible programarlas antes. La recolección de datos de los ciudadanos de la provincia de Santa Elena se llevó a cabo mediante cuestionarios en Google Formularios, alcanzando exitosamente la meta de 400 participantes.

A las personas que se entrevistó de manera presencial, como a los jueces y la ciudadana, se les solicitó firmar su consentimiento para poder grabarles la voz, mientras que a las personas que se les entrevistó a través de zoom se les solicitó su autorización para grabarles la voz de manera oral, el representante de una de las empresas privadas solicitó quedar en anónimo, debido a las implicaciones que podían acarrear la información que iba a otorgar.

En la entrevista realizada a segundo funcionario de la entidad privada se nos hizo la solicitud de que se mantuviera anónimo, debido a que su labor y la información otorgada es de tanta valía, ya que sus propios jefes se presentaron reacios a que se realizara la entrevista, no obstante, el ingeniero con el fin de desarrollar nuevos conocimientos, por lo que era su única condición para aceptar la entrevista.

3.4 Operacionalización de variables

CUADRO 3 OPERACIONALIZACIÓN

Titulo	Concepto	Dimensiones	Indicadores	Ítems	Técnica
Consentimiento en el uso de datos sensibles y la ley orgánica de protección de datos en el ámbito privado, 2023	**Variable dependiente** Consentimiento en el uso de datos sensibles El consentimiento en el uso de datos sensibles se refiere a la autorización explícita que una persona otorga para que sus datos sensibles sean recopilados, procesados y utilizados por una entidad específica, de acuerdo con ciertas	Protección de los datos sensibles	Analizar el reconocimiento del derecho humano a la protección de datos	¿Conoce cuáles son sus datos/información sensible?	cuestionario estructurado dirigido a la ciudadanía
			Evaluar el control absoluto sobre los datos sensibles y personales	¿Podría compartir con nosotros su experiencia específica sobre la utilización fraudulenta de sus datos sensibles?	Guía de entrevista dirigida a la ciudadanía
				¿Cuáles fueron las principales consecuencias que enfrentó como resultado del robo de identidad y el uso fraudulento de sus datos?	
		El consentimiento un derecho en la transacción contractual	Examinar el consentimiento en los contratos	Sabe ud si sus datos personales o el de alguno de sus conocidos han sido utilizados con otros propósitos por parte de empresas a las que se les entregó sus datos	cuestionario estructurado dirigido a la ciudadanía
				Cuando usted cede a la compra de un bien o servicio y entrega datos personales es requerido su consentimiento	
				Te resultan claros los términos y condiciones sobre la protección de datos?	
				¿Lee usted los términos y condiciones cuando las entidades o plataformas le piden su consentimiento?	
				¿Cómo obtiene la empresa el consentimiento de los usuarios para utilizar sus datos sensibles?	Guía de entrevista dirigida a la ciudadanía
			Investigar sobre la importancia de los elementos del consentimiento	¿Considera que la falta de desarrollo de los elementos del consentimiento establecidos en el artículo 8 de la Ley Orgánica de protección de datos vulnera el derecho a la protección de datos?	Guía de entrevista dirigida a Jueces

	condiciones y propósitos previamente establecidos.	La confidencialidad en la era de las Tics.	Identificar los riesgos de la Privacidad	¿Ha podido identificar cómo o dónde se produjo la brecha de seguridad que permitió que sus datos fueran comprometidos?	Guía de entrevista dirigida a la ciudadanía
				¿Ha recibido alguna compensación o reparación por los daños sufridos como resultado del robo de identidad y el uso fraudulento de sus datos?	
				¿Cómo describiría su nivel de confianza en las empresas y organizaciones que manejan y almacenan datos sensibles después de lo sucedido?	
				¿Cree que hay aspectos específicos de la regulación de protección de datos que podrían mejorarse para prevenir casos como el suyo en el futuro?	
			Comprender la importancia de la seguridad de Datos en entorno a las entidades Empresariales.	Conoce ud que toda empresa que obtiene datos sensibles de sus clientes debe declarar los términos y condiciones de su uso	cuestionario estructurado dirigido a la ciudadanía
				Sabías que si tus datos sensibles se utilizan para otro propósito sin tu autorización, se estarían vulnerando tus derechos a la protección de datos	
				¿Ha podido identificar cómo o dónde se produjo la brecha de seguridad que permitió que sus datos fueran comprometidos?	Guía de entrevista dirigida a la ciudadanía
				¿Ha recibido alguna compensación o reparación por los daños sufridos como resultado del uso fraudulento de sus datos?	
				¿Cómo describiría su nivel de confianza en las empresas y organizaciones que manejan y almacenan datos sensibles después de lo sucedido?	
				¿Cree que hay aspectos específicos de la regulación de protección de datos que podrían mejorarse para prevenir casos como el suyo en el futuro?	
Consentimiento en el uso de datos sensibles y la ley orgánica de protección de datos personales	**Variable independiente** La Ley Orgánica De Protección De Datos Personales En El	Constitución Del Ecuador	Derechos de libertad reconocidos en la constitución y aplicables a la protección de datos sensibles entre personas y entes privados	¿Cuáles son los principales problemas de la relación que existe entre el derecho a la protección de datos y el consentimiento al entregar los datos sensibles?	Guía de entrevista dirigida a Jueces
				¿Según su experiencia cuál considera son los procedimientos más eficaces para que los ciudadanos puedan acceder a la actualización, rectificación, eliminación o anulación de los datos sensibles? Previo a ejercer el habeas data	
				¿En el ejercicio de su profesión cuales han sido los casos más relevantes que ha manejado en torno a las vulneraciones al consentimiento en el uso de los datos personales?	

en el ámbito privado, 2023	Ámbito Privado Es una normativa que establece reglas y principios para proteger la privacidad de los individuos en relación con el tratamiento de sus datos personales por parte de entidades públicas y privadas.	Ley Orgánica De Protección De Datos Personales	El Consentimiento Informado: Pilar Fundamental en la Protección de Datos Personales	¿Cuáles son las implicaciones del principio de consentimiento informado en situaciones donde los datos personales se recopilan a través de dispositivos de IoT (Internet de las cosas) y otros dispositivos conectados, donde el consentimiento puede no ser directamente otorgado por los usuarios?	Guía de entrevista dirigida a funcionario de la Dinarp
			Sensibilidad: Ética y Regulación en el Tratamiento de Datos Sensibles"	¿Cuáles son los tipos de datos sensibles que su empresa recopila de los usuarios?	Guía de entrevista dirigida a funcionario de Claro
				¿Cómo obtiene la empresa el consentimiento de los usuarios para utilizar sus datos sensibles?	
				¿Qué políticas tiene la empresa en relación con el consentimiento y el uso de datos sensibles?	
				¿Cómo se almacenan y protegen los datos sensibles de los usuarios?	
				¿La empresa comparte los datos sensibles de los usuarios con terceros? En caso afirmativo, ¿cómo se aseguran de que se respeten las normas de privacidad?	
				¿Qué procedimientos tiene la empresa en caso de violaciones de datos o brechas de seguridad?	
				¿La empresa realiza evaluaciones periódicas de riesgos de privacidad? En caso afirmativo, ¿cómo se llevan a cabo?	
		Reglamento De Ley Orgánica De Protección De Datos Personales	Consentimiento y Tratamiento de Datos Sensibles: Responsabilidades Normativas	¿Cuál es la estructura organizativa de su entidad en relación con la protección de datos sensibles? ¿Cómo se dividen en departamentos o áreas y cuál es el papel de cada una en asegurar la seguridad y privacidad de esta información?	Guía de entrevista dirigida a funcionario de la Dinarp
				¿Cuáles son los procedimientos establecidos para garantizar la seguridad y privacidad de los datos sensibles de las personas?	
				¿Qué mecanismos del estado existen para garantizar que los titulares de datos estén informados sobre las finalidades del tratamiento de sus datos?	
				¿Qué medidas toman en caso de que se produzca una vulneración de datos?	
				¿Podrían compartir ejemplos específicos de cómo han abordado tales situaciones en el pasado?	
				¿Sabías que si tus datos sensibles se utilizan para otro propósito sin tu autorización, se estarían vulnerando tus derechos a la protección de datos?	Cuestionario estructurado dirigido a la ciudadanía
				Sabía ud que tiene el derecho a revocar el consentimiento de uso de datos personales por parte de empresas privadas	

Elaborado por: Luz Borbor y Wilson Chaca

CAPÍTULO IV
4. RESULTADOS Y DISCUSIÓN

4.1 Análisis, interpretación y discusión de resultados

2.1.1 Encuesta a ciudadanos de la provincia de Santa Elena.

Pregunta 1: ¿Conoce cuáles son sus datos/información sensible?

CUADRO 4 PREGUNTA 1

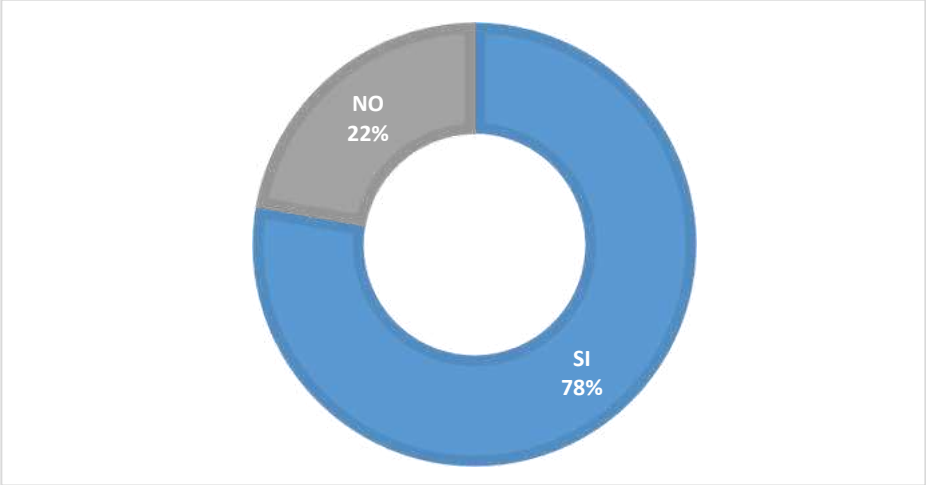
¿Conoce cuáles son sus datos/información sensible?

Valoración	Frecuencia	Porcentaje
Si	311	78%
No	89	22%
Resultados	400	100%

Elaborado por: Luz Borbor y Wilson Chaca - Fuente: Encuesta realizada a ciudadanos

GRÁFICO 5 PREGUNTA 1

¿Conoce cuáles son sus datos/información sensible?



Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Encuesta realizada a ciudadanos

Análisis

Esta pregunta busca determinar el nivel de conocimiento de las personas acerca de lo que constituye su información sensible. Dentro de la provincia de Santa Elena, de acuerdo con los datos recolectados de 400 encuestas, se ha revelado que el 78% de esta muestra, si conoce. Este valor nos indica que las personas, tienen conocimiento de que se requiere un mayor nivel de protección sobre nuestros datos personales. Este conocimiento refleja un avance significativo en la concientización y comprensión de los derechos de privacidad y protección de datos. Sin embargo, es necesario implementar medidas para cerrar la brecha informativa en cuanto a los ciudadanos que no tienen este conocimiento.

Pregunta 2: ¿Conoce usted que toda empresa que obtiene datos sensibles de sus clientes debe declarar los términos y condiciones de su uso?

CUADRO 5 PREGUNTA 2

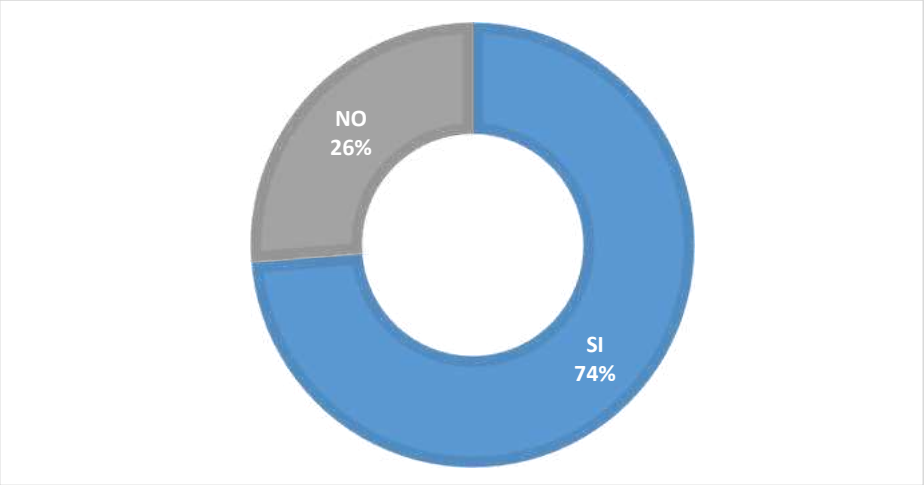
¿Conoce que toda empresa debe declarar los términos y condiciones del uso de datos sensibles?

Valoración	Frecuencia	Porcentaje
Si	295	74%
No	105	26%
Resultados	400	100%

Elaborado por: Luz Borbor y Wilson Chaca - Fuente: Encuesta realizada a ciudadanos

GRÁFICO 6 PREGUNTA 2

¿Conoce que toda empresa debe declarar los términos y condiciones del uso de datos sensibles?



Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Encuesta realizada a ciudadanos

Análisis

esta pregunta analiza si las personas conocen si las empresas recopilan información sensible de sus clientes. De acuerdo con el resultado de la encuesta, se puede observar que el 74% de los encuestados está informado sobre la obligación que tienen las empresas de declarar los términos y condiciones del uso de datos sensibles, esto permite una correcta aplicación de las normativas y garantiza la transparencia y el control sobre el uso de información sensible de los ciudadanos. Por el contrario, el 26% de la muestra denota una falta de conocimiento respecto a este derecho, situación que es preocupante, dado que presenta un riesgo de que sus derechos sean vulnerados por el desconocimiento de la protección legal de la que disponen. El conocimiento de los derechos y obligaciones relacionados con la protección de datos es relevante para la aplicación efectiva de las leyes, ya que, cuando los ciudadanos están informados, pueden exigir el cumplimiento de las normativas y actuar contra las infracciones. Por tanto, estas empresas estarían más incentivadas a cumplir con sus obligaciones legales.

Pregunta 3: ¿Cuándo usted cede a la compra de un bien o servicio y entrega datos personales es requerido su consentimiento?

CUADRO 6 PREGUNTA 3

Es requerido su consentimiento para el uso de su información cuando compra un bien o servicio

Valoración	Frecuencia	Porcentaje
Siempre	236	59%
Nunca	14	3%
A veces	150	38%
Resultados	400	100%

Elaborado por: Luz Borbor y Wilson Chaca - Fuente: Encuesta realizada a ciudadanos

GRÁFICO 7 PREGUNTA 3

Es requerido su consentimiento para el uso de su información cuando compra un bien o servicio

Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Encuesta realizada a ciudadanos

Análisis

Esta pregunta busca determinar si el encuestado es consciente de que al adquirir un bien o servicio y proporcionar sus datos personales, las empresas deben solicitar su consentimiento explícito para utilizar esos datos. Resulta que de 400 personas, 236 indicaron que siempre les solicitan, 150 que a veces y 14 que nunca les han pedido su consentimiento al momento de realizar la compra. Estos resultados indican una práctica inconsistente en la recolección del consentimiento por parte de las empresas, ya que la Ley Orgánica de Protección de Datos establece que las entidades deben obtener el consentimiento explícito de los individuos antes de realizar el tratamiento de sus datos. El hecho de que solo el 59% de los encuestados exprese que siempre se les ha pedido su autorización implica que el 41% de las empresas podrían estar incumpliendo las regulaciones vigentes. Esta situación sugiere una deficiencia en la aplicación de las normativas de protección de datos, lo que resulta en una vulneración de los derechos fundamentales de los individuos.

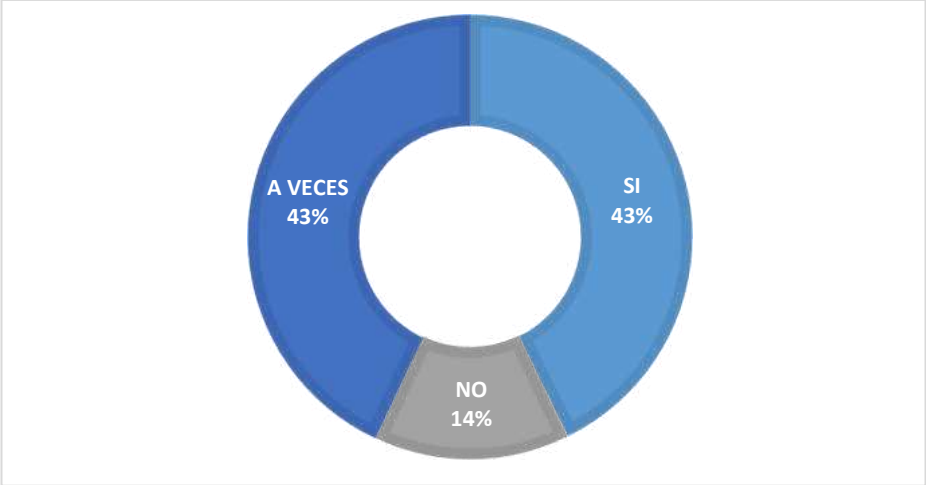
Pregunta 4: ¿Lee usted los términos y condiciones cuando las entidades o plataformas le piden su consentimiento?

CUADRO 7 PREGUNTA 4
¿Lee usted los términos y condiciones cuando le piden su consentimiento?

Valoración	Frecuencia	Porcentaje
Si	171	43%
No	57	14%
A veces	172	43%
Resultados	400	100%

Elaborado por: Luz Borbor y Wilson Chaca - Fuente: Encuesta realizada a ciudadanos

GRÁFICO 8 PREGUNTA 4
¿Lee usted los términos y condiciones cuando le piden su consentimiento?



Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Encuesta realizada a ciudadanos

Análisis

Indaga sobre si la persona revisa los términos y condiciones antes de otorgar su consentimiento en diversas plataformas o con distintas entidades. Los resultados muestran que el 43% de las personas respondieron afirmativamente, mientras que el 14% dijeron que no y el 43% que leen ocasionalmente o a veces. Estos resultados evidencian la diversidad de comportamientos entre los usuarios respecto a la lectura de términos y condiciones, y reconocer que la responsabilidad recae tanto en la empresa o entidad privada como en el cliente. Si bien es deber de la empresa proporcionar información comprensible sobre los términos del contrato, el cliente también tiene la responsabilidad de informarse adecuadamente sobre el mismo. El hecho de que una parte significativa de los encuestados no lea los términos y condiciones o lo haga ocasionalmente sugiere una falta de conciencia sobre las responsabilidades legales que tienen cuando realizan un contrato.

Pregunta 5: ¿Te resultan claros los términos y condiciones sobre la protección de datos?

CUADRO 8 PREGUNTA 5

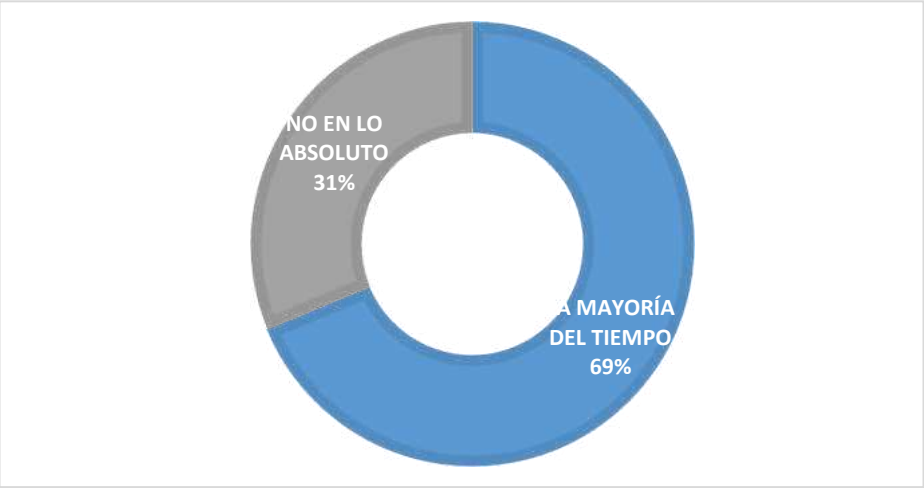
¿Te resultan claros los términos y condiciones sobre la protección de datos?

Valoración	Frecuencia	Porcentaje
La mayoría del tiempo	275	69%
No en lo absoluto	125	31%
Resultados	400	100%

Elaborado por: Luz Borbor y Wilson Chaca - Fuente: Encuesta realizada a ciudadanos

GRÁFICO 9 PREGUNTA 5

¿Te resultan claros los términos y condiciones sobre la protección de datos?



Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Encuesta realizada a ciudadanos

Análisis

Busca determinar si la persona encuentra comprensibles los términos y condiciones relacionados con la protección de datos cuando interactúa con diferentes plataformas, servicios o entidades. El 69% de la muestra indicó que la mayoría del tiempo les resultan claros, mientras que el 31% indicaron que no entienden lo que firman en lo absoluto. Este hallazgo pone en tela de duda un aspecto fundamental del consentimiento que debe establecerse dentro de los contratos para garantizar que las personas comprendan lo que están firmando. Uno de estos elementos es que debe ser informado, es decir, debe estar la información completa y comprensible sobre cómo se utilizarán sus datos antes de su tratamiento, y otro elemento es que debe ser inequívoca, lo que comprende que no debe existir duda ni ambigüedad acerca del tratamiento de esta información. Estos resultados revelan que en ciertos contratos dentro de algunas entidades privadas no se cumplen con los elementos intrínsecos del consentimiento establecidos desde el código civil.

Pregunta 6: ¿Sabías que si tus datos sensibles se utilizan para otro propósito sin tu autorización, se estarían vulnerando tus derechos a la protección de datos?

CUADRO 9 PREGUNTA 6

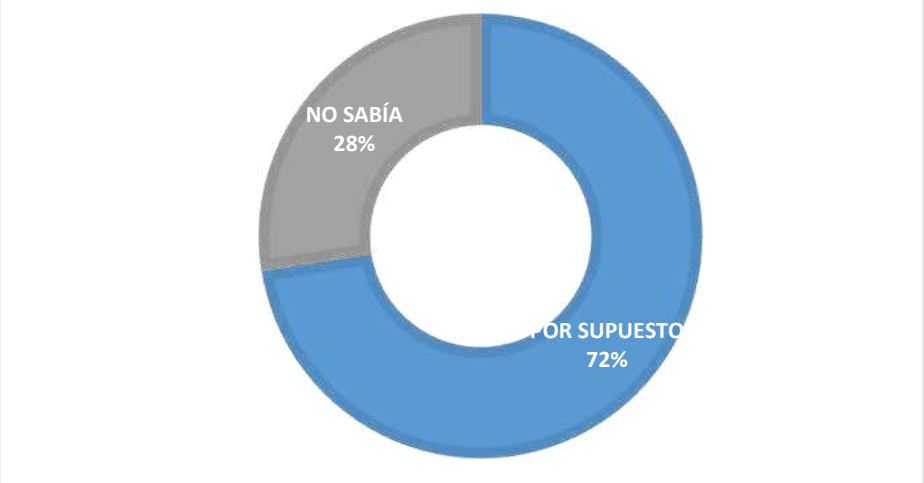
¿Sabías que se vulneran tus derechos si usan tu información para otro propósito sin tu autorización?

Valoración	Frecuencia	Porcentaje
Por supuesto	290	72%
No sabía	110	28%
Resultados	400	100%

Elaborado por: Luz Borbor y Wilson Chaca - Fuente: Encuesta realizada a ciudadanos

GRÁFICO 10 PREGUNTA 6

¿Sabías que se vulneran tus derechos si usan tu información para otro propósito sin tu autorización?



Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Encuesta realizada a ciudadanos

Análisis

Busca determinar si el encuestado está consciente de que el uso de sus datos sensibles para fines distintos a los autorizados constituye una violación de sus derechos a la protección de datos. Los resultados muestran que el 72% de las personas encuestadas demuestran tener conocimiento sobre si el uso indebido de sus datos sensibles se da por parte de empresas privadas, lo cual les estaría vulnerando sus derechos. Este grupo de personas comprende que cualquier desviación en el uso de sus datos sensibles, que no esté alineada con el propósito acordado, constituye una vulneración a sus derechos. Sin embargo, el 28% restante carece de este conocimiento, lo cual conlleva a que la falta de conciencia sobre sus derechos exponga una brecha significativa en la comprensión legal y podría traer consecuencias como abusos por parte de estas empresas relacionados con el manejo de datos. Esta disparidad subraya la importancia de una educación continua sobre nuestra privacidad y el papel de las autoridades en informar a la población sobre sus derechos y responsabilidades en el ámbito digital.

Pregunta 7: ¿Sabía usted que tiene el derecho a revocar el consentimiento de uso de datos personales por parte de empresas privadas?

CUADRO 10 PREGUNTA 7

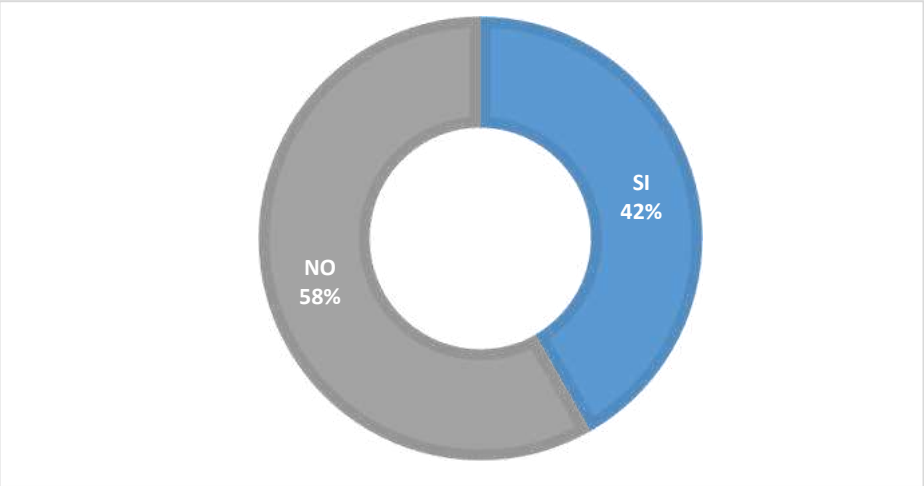
¿Sabía que puede revocar el consentimiento de uso de su información por parte de empresas privadas?

Valoración	Frecuencia	Porcentaje
Si	167	42%
No	233	58%
Resultados	400	100%

Elaborado por: Luz Borbor y Wilson Chaca - Fuente: Encuesta realizada a ciudadanos

GRÁFICO 11 PREGUNTA 7

¿Sabía que puede revocar el consentimiento de uso de su información por parte de empresas privadas?



Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Encuesta realizada a ciudadanos

Análisis

busca determinar si el encuestado está al tanto de su derecho a retirar el consentimiento para el uso de su información por parte de empresas privadas. De los 400 encuestados, el 42% indicaron estar al tanto de la posibilidad de revocar el consentimiento. Sin embargo, el 58% desconocía esta información. Esto sugiere una deficiencia en la comunicación por parte de las empresas al momento de establecer los contratos de servicios o ventas. La falta de claridad en los términos y condiciones relativos a los datos personales y sensibles, específicamente en lo que respecta a la revocación del consentimiento. Estos resultados plantean interrogantes sobre la transparencia y el cumplimiento de las obligaciones legales por parte de las empresas en cuanto a la protección de datos y sugiere la necesidad de una mayor regulación y supervisión para garantizar que las empresas proporcionen información completa y comprensible sobre el tratamiento de los datos personales, incluyendo la posibilidad de revocar el consentimiento en cualquier momento.

Pregunta 8: ¿Sabe usted si sus datos personales o el de alguno de sus conocidos han sido utilizados con otros propósitos por parte de empresas a las que se les entregó sus datos?

CUADRO 11 PREGUNTA 8

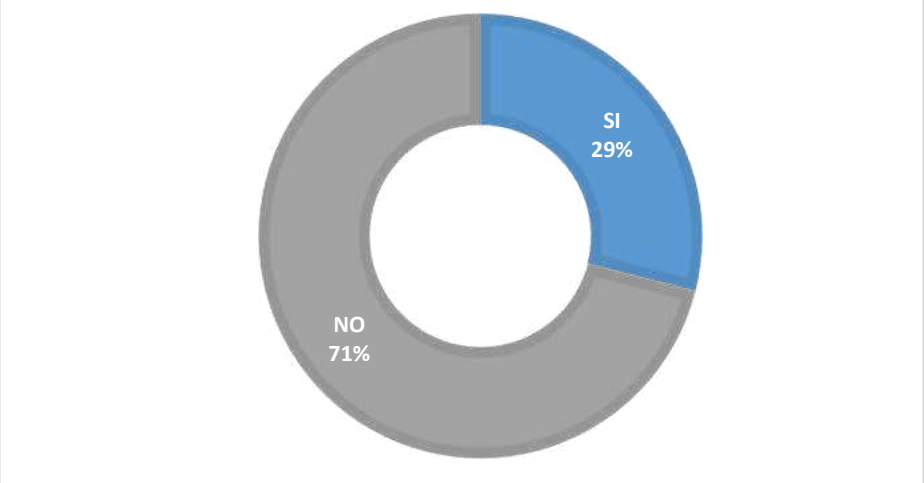
¿Sabe si sus datos personales o el de alguno de sus conocidos han sido utilizados con otros propósitos?

Valoración	Frecuencia	Porcentaje
Si	116	29%
No	284	71%
Resultados	400	100%

Elaborado por: Luz Borbor y Wilson Chaca - Fuente: Encuesta realizada a ciudadanos

GRÁFICO 12 PREGUNTA 8

¿Sabe si sus datos personales o el de alguno de sus conocidos han sido utilizados con otros propósitos?



Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Encuesta realizada a ciudadanos

Análisis

Busca determinar si el encuestado tiene conocimiento de casos en los que sus propios datos personales o los de personas cercanas hayan sido utilizados por empresas para fines distintos a los autorizados inicialmente. El 29% de la población respondió afirmativamente, es decir, 116 personas de las 400 encuestadas. El 71% respondió que no. Esta información revela que, a pesar de la existencia de la ley orgánica de protección de datos y su reglamento, que supuestamente protegen a las personas del uso indebido de su información, estas malas prácticas siguen ocurriendo, especialmente por parte de empresas privadas. El hecho de que casi un tercio de los encuestados haya experimentado un uso indebido de sus datos personales indica que las empresas parecen estar evadiendo las regulaciones establecidas y continúan vulnerando el derecho a la privacidad de sus usuarios al compartir esta información con terceros o utilizarla de manera inapropiada. Esto pone en evidencia la necesidad de una mayor implementación y vigilancia en las leyes de protección de datos.

2.1.2 Análisis de Entrevista dirigida a Juez de Primer Nivel.

Nombre del entrevistado: Ab. Juan Carlos Camacho Flores

Fecha de la entrevista: Miércoles 22 de mayo de 2024

Lugar de la entrevista: Consejo de la Judicatura De Santa Elena

Pregunta #1 ¿Cuáles son los principales problemas de la relación que existe entre el derecho a la protección de datos y el consentimiento al entregar los datos sensibles?

El consentimiento, definido como la facultad de adquirir responsabilidades y contraer obligaciones, debe ser libre e informado para ser válido. La capacidad para dar consentimiento se adquiere generalmente a los 18 años, el problema surge cuando el consentimiento no es libre e informado, los vicios del consentimiento, como el error, la fuerza y el dolo, pueden invalidar el mismo. Los contratos se consideran ley para las partes. Sin embargo, la complejidad de los términos y condiciones puede dificultar que los ciudadanos comprendan completamente lo que están autorizando, la ley también permite la revocación del consentimiento en cualquier momento, al igual que exige que el consentimiento sea inequívoco, es decir, que no presente dudas sobre su alcance. Sin embargo, la normativa no especifica cómo lograr esto en contratos digitales, como en los contratos de adhesión. Respecto a si hay "fuerza" en los contratos de adhesión de grandes empresas tecnológicas, que ofrecen servicios casi indispensables, no se considera fuerza en el sentido legal, ya que no hay coerción física, aunque se reconoce que pueden plantear problemas de comprensión para los usuarios.

Pregunta #2 ¿Considera que la falta de desarrollo de los elementos del consentimiento establecidos en el artículo 8 de la Ley Orgánica de protección de datos vulnera el derecho a la protección de datos?

El artículo 8 de la Ley Orgánica de protección de datos establece principios que recuerdan a los del Código Civil, haciendo hincapié en la libertad, la información y la revocación del consentimiento. Es interesante notar que el código civil ya contemplaba la necesidad de un consentimiento informado y la capacidad para otorgarlo, que es fundamental, especialmente en casos que involucran a menores de edad, quienes carecen de la capacidad legal para otorgar consentimiento, la verificación de la edad y la capacidad de los usuarios puede ser problema, en plena era digital. Hay una situación en la que, desde mi punto de vista, falta legislar en cuanto el desarrollo de estas plataformas, no es un tema de esta ley, sino de otras

leyes que permitan el funcionamiento de estas plataformas aquí en el país, si nosotros regulamos el funcionamiento de las plataformas en el país a través de la Ley De Telecomunicaciones o a través de la Ley De Manejo De Datos Públicos en relación con la capacidad de las personas, porque ahí se establece que tienen la capacidad de registrar todos los datos de las personas como el registro civil. Entonces, sabemos que a través de estos datos una persona que ingresa a las plataformas hay un cruce de información con las entidades de control, con la ley se regula el funcionamiento de estas plataformas, entonces ahí si vamos a ver todos los elementos que constan en el art 8 están bien enmarcados, porque solo las personas que tengan la capacidad podrán autorizar o no la utilización de sus datos personales, de lo contrario, automáticamente dichos contratos quedarían sin efecto, bloqueados, quedarían invalidados

Pregunta #3 ¿Según su experiencia cuál considera son los procedimientos más eficaces para que los ciudadanos puedan acceder a la actualización, rectificación, eliminación o anulación de los datos sensibles? Previo a ejercer el habeas data

Como establece la Constitución, el derecho a la rectificación se regula en términos generales a través del habeas data. Sin embargo, antes de llegar a esa instancia, tenemos normas como el Código Civil en las que podríamos implementar la mediación como medida alternativa, en la cual se solicita la rectificación de esos datos, indicando cuál ha sido la afectación que ha sufrido la persona. Más allá de eso, no hay otra opción. Podemos utilizar el ejemplo de las redes sociales, que no están sometidas a ninguna legislación específica. ¿Cómo podemos hacer que se rectifiquen esos datos?, si en los mismos contratos de adhesión muchas veces se estipula que deben someterse a las leyes del país de origen de la plataforma

Pregunta #4 ¿En el ejercicio de su profesión cuales han sido los casos más relevantes que ha manejado en torno a las vulneraciones al consentimiento en el uso de los datos personales?

Existe una sentencia de la Corte Constitucional, si mal no recuerdo, que hace referencia a que los datos de las personas involucradas en delitos pueden estar ocultos, hemos tenido muchos casos de personas que han sido sentenciadas, pero no quieren que esos datos consten en el sistema SATJE, el cual es un sistema que maneja el Consejo de la Judicatura para la información de todas estas personas que han sido parte de procesos judiciales. Estas personas han solicitado que se oculten estos datos. Para ello, el Consejo de la Judicatura ya emitió una

resolución especificando el procedimiento para el ocultamiento o la corrección de estos datos.

Pregunta #5 Sabiendo que los datos en la era digital se han convertido en los activos más valiosos de las empresas privadas, ¿Cómo se establecería la reparación integral si la entidad privada se niega a dejar de usar y almacenar, luego de que se haya solicitado por la vía de comunicación idónea la revocatoria del consentimiento?

La reparación puede ser material e inmaterial. La reparación material se refiere a los daños y perjuicios ocasionados por el uso indebido de datos personales. En este sentido, no está establecido en ninguna norma cómo se debe cuantificar este daño, salvo en materia civil, donde se puede cuantificar el daño moral, en que se debe demostrar cómo la utilización de esos datos personales ha afectado el entorno social. En materia constitucional, la reparación material estaría a la sana crítica del juez, ya que no hay un parámetro establecido, podría apoyarse en el código civil para evaluar el daño y perjuicio, y cómo quedó afectada la reputación de la persona. En cuanto a la reparación inmaterial, podría incluir disculpas públicas y la rectificación de los datos en la plataforma. Estas serían las reparaciones integrales que establece la Ley Orgánica de Garantías Constitucionales.

Análisis

Se destaca que el consentimiento debe ser libre e informado para ser válido, lo que implica que debe otorgarse de manera voluntaria, sin coerción. Las personas deben decidir por sí mismas si desean compartir su información. Además de ser informado, el consentimiento debe implicar recibir información transparente, clara, comprensible y sin barreras técnicas sobre cómo se utilizarán los datos y cómo se tratarán, con la posibilidad de revocarlo en cualquier momento. Incluyendo que entre los otros elementos del consentimiento se encuentran que debe ser específico, es decir, el uso previsto de la información debe ser sin ambigüedades. Las entidades privadas que emplean prácticas como términos y condiciones excesivamente extensos o poco comprensibles incurren en un vicio del consentimiento, como el dolo, al aprovecharse de la falta de comprensión de las personas. Se plantea también la problemática de los contratos de adhesión, donde se establecen condiciones que no pueden ser modificadas por la otra parte, otorgando un poder desequilibrado a la entidad privada, ya que el usuario o consumidor no tiene capacidad real de negociación, ya que pueden contener cláusulas complejas o abusivas, que dificultan su comprensión por parte del consumidor, lo

que refuerza el poder de la parte más fuerte. Y aunque no existe coerción física, el monopolio de algunos servicios complica la situación, ya que los consumidores pueden sentirse obligados a aceptar condiciones desfavorables para acceder al servicio.

2.1.3 Análisis de Entrevista dirigida a Juez de Primer Nivel.

Nombre del entrevistado: Ab. Richard Fabián Gavilanes Briones.

Fecha de la entrevista: Miércoles, 21 de mayo de 2024

Lugar de la entrevista: Consejo de la Judicatura De Santa Elena

Pregunta #1 ¿Cuáles son los principales problemas de la relación que existe entre el derecho a la protección de datos y el consentimiento al entregar los datos sensibles?

El primer problema de esta relación es la falta de información que nace de la falta de cultura de leer, de informar, supuestamente si no estoy informado es porque no tengo el hábito de la lectura, de leer y sobre todo de informarme al respecto sobre esta temática, el limitante dentro de esta relación es la falta de información adecuada, idónea y profunda sobre el tema y las consecuencias, pros y contras que puede derivar de esta relación. Por experiencia personal, la mayoría de los contratos son complejos y tienen una serie de requerimientos que por la extensión dificulta que las personas los lean por completo. Conforme la Ley Orgánica de Protección de Datos, para evitar este problema, los contratos deben ser breves, ágiles y sencillos, sin tantas complicaciones. Es necesario aplicar verdaderamente la sencillez, la rapidez, la fluidez y, sin tanto formalismo, ese es el término, para evitar la falta de información completa de la persona interesada.

Pregunta #2 ¿Considera que la falta de desarrollo de los elementos del consentimiento establecidos en el artículo 8 de la Ley Orgánica de protección de datos vulnera el derecho a la protección de datos?

Justamente como indicaba respecto a la primera pregunta, esto va dirigido a personas adultas. Uno se compromete, pues tiene que darse cuenta de que, así como exige derechos, también debe cumplir con sus obligaciones. No creo que exista una afectación, porque si vas a dar consentimiento, lo haces de forma libre, espontánea, directa y sin ninguna coacción, si no se advierten esos elementos y no hay amenaza o intimidación. Si pasa lo contrario, existe una vulneración, ya que no lo hace de forma consciente, libre y voluntaria. Los tres aspectos que se deben tomar en cuenta en la voluntariedad para consentir en este tipo de relaciones: que sea libre, hecho por personas capaces, y sin ninguna coacción de ninguna clase.

Pregunta #3 ¿Según su experiencia cuál considera son los procedimientos más eficaces para que los ciudadanos puedan acceder a la actualización, rectificación, eliminación o anulación de los datos sensibles? Previo a ejercer el habeas data

El Consejo de la Judicatura, mediante una resolución, ya nos dio las pautas y el reglamento a seguir cuando se pide la ratificación o eliminación de datos que no siempre se debe recurrir al habeas data como garantía jurisdiccional, sino que en ese caso de datos erróneos dentro de la función judicial respecto de determinada demanda, se lo haga mediante esa resolución expedida por el pleno Consejo de la Judicatura en 2023. Como experiencia propia aquí respecto de los datos errados del registro civil, siempre ocurren, con esos errores agotan la vía administrativa, que es el primer formalismo y luego les obligan a acudir a la vía judicial. Entonces, si bien es cierto, la Constitución dice que las instituciones deben tener un reglamento interno desde la fase administrativa para la corrección de sus datos, no se lo hace. Cuando se lleva a la vía judicial, no es tan célere como el habeas data, demora justamente porque no tienen un procedimiento propio, se las presenta en el procedimiento ordinario según Cogep. El Habeas data es más célere, tiene un trámite ágil, rápido, sencillo, eficaz, informal, ni siquiera se presenta la demanda escrita y sino oral y el juez la debe acoger, calificar y resolver lo que corresponde.

Pregunta #4 ¿En el ejercicio de su profesión cuales han sido los casos más relevantes que ha manejado en torno a las vulneraciones al consentimiento en el uso de los datos personales?

No he tenido un caso relevante como tal, pero en Quito tuve una experiencia mientras estaba como secretario encargado. Era una unión de hecho entre una pareja del mismo sexo, cuando recién comenzó el tema de la Constitución y los derechos de avanzada. La Corte Constitucional todavía no se había pronunciado al respecto sobre el artículo del Código Civil relativo al matrimonio. Nos tomó un poco por sorpresa, ya que no había jurisprudencia desarrollada. Como les digo, nos cogió desprevenidos, la jueza superior, con la que trabajaba, tenía cierta repulsión a conocer este juicio, no quería darle trámite. Esto demuestra que cuando uno no se informa y no se empodera de los principios y derechos de esos grupos que también consagra la Constitución, provocamos por acción u omisión, vulneraciones.

Pregunta #5 Sabiendo que los datos en la era digital se han convertido en los activos más valiosos de las empresas privadas, ¿Cómo se establecería la reparación integral si la entidad

privada se niega a dejar de usar y almacenar, luego de que se haya solicitado por la vía de comunicación idónea la revocatoria del consentimiento?

Yo creo que en este caso se debería activar la garantía del habeas data o algún trámite administrativo entre particulares. Si ya se rompe el esquema y se altera el principio de reserva del consentimiento, y tampoco se da paso a la revocatoria de ese consentimiento, se produce una afectación mayor. Esta situación justifica recurrir a una de las garantías jurisdiccionales contempladas en la Constitución, ya que estas garantías son justamente las vías más rápidas e idóneas cuando ocurre esto, especialmente en la relación entre un particular y una empresa. Imaginemos lo que implica enfrentarse a una empresa de gran tamaño, como una farmacéutica, un particular que consintió en dar sus datos sensibles se encuentra en una posición de desigualdad frente a la multinacional, en estos casos, existen garantías para equilibrar la situación y permitir al particular enfrentarse a la empresa. La reparación integral debería incluir el cese de la difusión de la información, pero esto no es suficiente porque ya se ha hecho un mal uso de los datos, una posible reparación inmaterial podría ser una disculpa pública, la cual debería ser publicada. Además, una reparación material, en forma de compensación económica, complementaría este tipo de reparaciones; no se trata solo de detener el uso de esa información por parte de la empresa. Deben implementarse otras medidas para asegurar que la afectación sea resarcida de manera íntegra y completa.

Análisis

A partir de la entrevista realizada, se destaca que uno de los principales problemas en la relación entre derechos de protección y consentimiento en relación con la transferencia de datos es la falta de información suficiente en los contratos. Si estos acuerdos son difíciles de leer o analizar, las personas a menudo no entienden completamente los términos, por lo que es necesaria una simplificación para aumentar la claridad y facilitar la comprensión del usuario. Esto es especialmente importante cuando se incluye la importancia y desarrollo de los elementos del consentimiento en el derecho civil y en la ley de protección de datos personales, que deben ser libres, específicos, informados e inequívocos. Además, se debe considerar la posibilidad de que las personas brinden su consentimiento informado sin coerción, ya que no desarrollar estos elementos puede violar los derechos de protección de datos al no brindar un consentimiento informado y voluntario. Un proceso rápido y eficiente para acceder y corregir datos confidenciales es esencial, especialmente en el dominio

público. Sin embargo, a pesar de la regulación del proceso administrativo, éste muchas veces no se lleva a cabo adecuadamente. En el caso del sector privado, existen dudas sobre cómo se realizan estos trámites. El hábeas data se proporciona como garantía de verificación y activación en caso de negativa a retirar el consentimiento después de que se haya violado un derecho. En este sentido, es deber del juez determinar el tipo de indemnización en caso de lesión que menoscabe la independencia de la persona.

Análisis de Entrevista dirigida a Juez de Primer Nivel.

Nombre del entrevistado: Ab. Ana María Tapia Blacio

Fecha de la entrevista: Miércoles, 22 de mayo de 2024

Lugar de la entrevista: Consejo de la Judicatura De Santa Elena

Pregunta #1 ¿Cuáles son los principales problemas de la relación que existe entre el derecho a la protección de datos y el consentimiento al entregar los datos sensibles?

El principal problema de la información personal es que accedemos a muchas plataformas en las que, inconscientemente, autorizamos la divulgación de nuestra información. Estas plataformas no tienen regulación, lo que dificulta exigir la reserva de información o evitar su divulgación. Como he indicado, estas plataformas a las que accedemos tal vez tienen sus reglamentos para acceder, con alguna aceptación oculta que uno aprueba sin conocer realmente cómo se va a manipular la información. Ya hay grupos a nivel mundial, no solo en nuestro país, que han levantado la voz acerca de la divulgación o difusión de información personal sin haberlo autorizado. Aunque en nuestro país existen normas que regulan esto, ¿cómo demandamos a Facebook? ¿cómo demandamos a Instagram? ¿cómo demandamos a Twitter? ¿En qué vía podríamos conseguir una reparación por esta vulneración?

Pregunta #2 ¿Considera que la falta de desarrollo de los elementos del consentimiento establecidos en el artículo 8 de la Ley Orgánica de protección de datos vulnera el derecho a la protección de datos?

Si, primero porque el ciudadano no conoce sus derechos esa es una de las cosas que más afectan. Si no conoces algo, no tienes como de exigirlo, el estado no tiene un mecanismo de difusión para decirle, usted puede decir que no, o usted debe de exigir esto. En nuestro país siempre se ha manejado con una legislación sancionadora, mas no preventiva. No tenemos ningún método para poder prevenir un sin número de actos que en temas generales sucede.

Pregunta #3 ¿Según su experiencia cuál considera son los procedimientos más eficaces para que los ciudadanos puedan acceder a la actualización, rectificación, eliminación o anulación de los datos sensibles? Previo a ejercer el habeas data

Bueno, si bien es cierto, previo al habeas data, uno debe demostrar haber solicitado la rectificación, las personas por el tema de informalidad, no lo realizan debidamente o por escrito o a través de un email, para poder tener una constancia de este reclamo porque si bien es cierto, la garantía constitucional, que ya claramente la conocen, la institución demandante tendrá que demostrar que no hizo la corrección, porque no tiene la obligación accionante de demostrarlo. Pero, lastimosamente, las instituciones públicas y privadas, porque aquí estamos hablando de datos personales que pueden ser información en el sector público y privado, no atienden estas peticiones, porque talvez el habeas data solamente exige la rectificación, mas no una sanción.

Pregunta #4 ¿En el ejercicio de su profesión cuales han sido los casos más relevantes que ha manejado en torno a las vulneraciones al consentimiento en el uso de los datos personales?

Relevante no creo que haya habido ninguno, de ahí, la mayoría de las acciones de habeas data que he visto son sobre la falta de contestación a la solicitud de información, pero de rectificación de datos personales no he tenido ninguna acción

Pregunta #5 Sabiendo que los datos en la era digital se han convertido en los activos más valiosos de las empresas privadas, ¿Cómo se establecería la reparación integral si la entidad privada se niega a dejar de usar y almacenar, luego de que se haya solicitado por la vía de comunicación idónea la revocatoria del consentimiento?

Bueno, para que haya sanción debe estar incluido en el código orgánico integral penal como un delito o como una contravención. Es necesario poder poner sanciones que puedan establecer de alguna manera esta reparación porque, si bien es cierto a través de habeas data pudiera conseguir una reparación integral, una indemnización por el daño causado, siempre y cuando se pueda demostrar, pero lastimosamente el ciudadano necesita tener una sanción para cumplir. Vivimos en una sociedad que a pesar de las sanciones drásticas que tenemos, un montón de contravenciones y delitos, la gente decide seguir cometiéndolos, pero, lamentablemente, ese es el actuar de todos nosotros.

Análisis.

La jueza destaca la falta de regulación en plataformas donde se divulga información personal sin un consentimiento claro por parte del usuario, que, a pesar de que existen normas que podrían regular esto, es difícil aplicarlas a nivel internacional. Esta situación genera incertidumbre sobre cómo garantizar la adecuada salvaguarda de la privacidad de los individuos en el ámbito digital, considerando especialmente las dificultades inherentes para aplicar normativas a nivel internacional. Además de esto, la falta de conocimiento por parte de los ciudadanos sobre sus derechos afecta su capacidad para exigir el consentimiento adecuado, lo que impide que puedan ejercer sus derechos de manera apropiada. Esta situación plantea que la ley es impositiva y no preventiva, ya que solo castiga, pero no advierte sobre la rectificación de datos, a la cual se puede recurrir. Sin embargo, se considera importante destacar que las instituciones, tanto públicas como privadas, a menudo no responden adecuadamente a las solicitudes, lo que representa un problema para el ciudadano en el momento en que necesita seguir este procedimiento. Se plantea la necesidad de sanciones efectivas, posiblemente incluyendo disposiciones en el código de procedimiento penal, para asegurar que las entidades privadas respeten los derechos de privacidad de los individuos. Destaca que la posibilidad de una sanción podría ser un incentivo efectivo para el cumplimiento de las leyes de protección de datos.

2.1.4 Análisis de Entrevista dirigida a entidad privada

Nombre del entrevistado: Ing. Priscila -Talento Humano Empresa Disnacon

Fecha de la entrevista: Lunes, 27 de mayo de 2024

Lugar de la entrevista: Zoom

Pregunta #1 ¿Cuáles son los tipos de datos sensibles que su empresa recopila de los usuarios?

Los datos sensibles como la etnia, la edad, sexo, esos son los datos que nosotros recopilamos normalmente que se debe tener de información básica de cada empleado.

Pregunta #2 ¿Cómo obtiene la empresa el consentimiento de los usuarios para utilizar sus datos sensibles?

De manera verbal los comunicamos con ellos, hacemos la entrevista, ellos nos facilitan la información y adicional se hace llenar una ficha.

Pregunta #3 ¿Qué políticas tiene la empresa en relación con el consentimiento y el uso de datos sensibles?

Normalmente no se puede otorgar información a terceras personas y eso está estipulado en el reglamento interno de la empresa. Está relacionada al reglamento del código de trabajo, entonces lo que nos indican los artículos del código de trabajo está relacionado al reglamento interno de la empresa.

Pregunta #4 ¿Cómo se almacenan y protegen los datos sensibles de los usuarios?

Pues se archiva. Hay un archivero para cada empleado, o sea, quieren saber información de esa persona, va al archivo y busca la carpeta de esa persona.

Pregunta #5 ¿La empresa comparte los datos sensibles de los usuarios con terceros? En caso afirmativo, ¿cómo se aseguran de que se respeten las normas de privacidad?

No.

Pregunta #6 ¿Qué procedimientos tiene la empresa en caso de violaciones de datos o brechas de seguridad?

Pues como le indicaba al principio, tienen que cumplir lo que dice en el reglamento y en el reglamento indica que no se puede otorgar información a terceros. Por cualquier situación se impone las sanciones que nos demanda el Código de Trabajo.

Pregunta #7 ¿La empresa realiza evaluaciones periódicas de riesgos de privacidad? En caso afirmativo, ¿cómo se llevan a cabo?

Pues digamos que periódicas no, pero cada seis meses o cada año sí se hace una evaluación de cómo está la información que cada uno tiene y cómo podemos actualizar la información o tenemos que realizar otro tipo de informativos para tener todo de acuerdo con cómo se debe establecer.

Análisis.

En relación con el tratamiento de datos que realiza esta empresa, especialmente la información de las personas a las que contrata, generalmente se maneja con sumo cuidado. Según sus declaraciones, se basa en la ley, especialmente en el código de trabajo. El consentimiento para el uso de su información se obtiene de manera verbal y escrita, mediante el llenado a mano de una ficha.

Jurídicamente, el consentimiento para el uso de datos sensibles debe ser explícito, informado y documentado adecuadamente, acorde con lo estipulado en el contrato. Esta entidad privada cuenta con políticas internas que prohíben la divulgación de estos datos a terceros, y se aplican las sanciones correspondientes en casos de vulnerabilidad potencial, conforme al código de trabajo. La empresa afirma no compartir datos sensibles con terceros, lo cual es congruente con los principios de minimización de datos y confidencialidad. En cuanto a las evaluaciones periódicas, que según menciona se realizan cada seis meses principalmente para la actualización de información, es un aspecto positivo. Sin embargo, para que estas evaluaciones sean realmente efectivas, deberían ser sistemáticas y exhaustivas, enfocándose en identificar y mitigar riesgos de manera continua.

2.1.5 Análisis de Entrevista dirigida a entidad privada

Nombre del entrevistado: Anónimo

Fecha de la entrevista: Martes, 28 de mayo de 2024

Lugar de la entrevista: Zoom

Pregunta #1 ¿Cuáles son los tipos de datos sensibles que su empresa recopila de los usuarios?

Nuestra empresa recopila diversos tipos de datos sensibles de los usuarios para ofrecer servicios personalizados y mejorar la calidad de nuestras ofertas. Entre estos datos se incluyen información personal básica como nombre, dirección y fecha de nacimiento. También recolectamos información de contacto, que comprende correos electrónicos y números de teléfono, lo cual nos permite comunicarnos de manera efectiva con nuestros clientes. En términos de datos financieros, recopilamos números de tarjeta de crédito y cuentas bancarias. Además, monitorizamos el historial de transacciones de los usuarios, identificando dónde y cómo utilizan sus tarjetas, ya sea en supermercados, tiendas específicas o en línea. Esta información nos permite realizar un seguimiento detallado de los hábitos de consumo y ofrecer descuentos y promociones relevantes. Adicionalmente, recopilamos información de salud que puede incluir el historial médico, registros de seguros y datos sobre visitas a centros de salud y hospitales. Esto se realiza para proporcionar servicios más personalizados y coordinar beneficios adicionales. Por último, también manejamos datos de identificación, como documentos de identidad e información biométrica

en ciertos casos, y obtenemos información adicional a través de alianzas con otras empresas, lo que nos ayuda a ofrecer paquetes de viajes y otros servicios personalizados.

Pregunta #2 ¿Cómo obtiene la empresa el consentimiento de los usuarios para utilizar sus datos sensibles?

Para obtener el consentimiento de los usuarios, nuestra empresa utiliza un formulario detallado que explica claramente cómo se utilizarán sus datos. Este formulario incluye una explicación sobre cómo el tratamiento de sus datos puede mejorar su historial crediticio y asegurar la fiabilidad al solicitar créditos en instituciones financieras. Es fundamental que los usuarios entiendan que su información será tratada de manera confidencial y en conformidad con las normativas legales vigentes. Además, cada año revisamos y actualizamos los contratos con los usuarios para asegurarnos de que están informados y de acuerdo con los nuevos usos que se darán a sus datos. Esta revisión incluye cualquier cambio en las políticas de privacidad y en los propósitos de uso de la información recopilada.

Pregunta #3 ¿Qué políticas tiene la empresa en relación con el consentimiento y el uso de datos sensibles?

Nuestra empresa ha implementado diversas políticas internas para gestionar de manera adecuada el consentimiento y el uso de los datos sensibles de los usuarios. Estas políticas incluyen reglas estrictas de privacidad, como las estipuladas en los estándares internacionales EDRP y SPA, los cuales seguimos conforme a las leyes de comunicación y datos de la Unión Europea.

Además, tenemos directrices claras sobre los deberes y sanciones para los responsables del tratamiento de datos. Estas sanciones pueden incluir desde amonestaciones hasta el despido, y en casos graves, pueden llevar a acciones legales. El departamento jurídico se encarga de supervisar el cumplimiento de estas políticas y de realizar auditorías periódicas para asegurar que se siguen los procedimientos adecuados.

En caso de violaciones de datos o brechas de seguridad, la empresa tiene protocolos establecidos para actuar rápidamente. Esto incluye la elaboración de informes detallados sobre la naturaleza de la violación y la implementación de medidas correctivas para mitigar cualquier daño.

Pregunta #4 ¿Cómo se almacenan y protegen los datos sensibles de los usuarios?

Nuestra empresa tiene un sistema detallado para almacenar y proteger los datos sensibles de los usuarios. La información personal, como nombres, direcciones y fechas de nacimiento, así como información de contacto, como correos electrónicos y números de teléfono, se almacenan en bases de datos seguras y encriptadas. Los datos financieros, incluidos los números de tarjetas de crédito y cuentas bancarias, se manejan con un nivel adicional de seguridad. Monitoreamos de cerca las transacciones para comprender mejor los patrones de uso de los usuarios y poder ofrecer promociones y descuentos relevantes.

Para proteger esta información, utilizamos una combinación de medidas de seguridad avanzadas, incluyendo encriptación de datos en múltiples niveles, controles de acceso estrictos y monitoreo constante de nuestras bases de datos. Además, implementamos procedimientos de seguridad que nos permiten detectar y responder rápidamente a cualquier intento de acceso no autorizado.

Pregunta #5 ¿La empresa comparte los datos sensibles de los usuarios con terceros? En caso afirmativo, ¿cómo se aseguran de que se respeten las normas de privacidad?

Sí, nuestra empresa comparte datos sensibles de los usuarios con terceros, pero siempre bajo estrictos contratos de confidencialidad. Antes de compartir cualquier información, evaluamos qué datos son necesarios para los terceros y establecemos acuerdos claros sobre su uso. Por ejemplo, compartimos información sobre las tarjetas de crédito utilizadas, las cuentas más empleadas, y las preferencias de contacto como correos electrónicos o números de teléfono.

Para asegurar que se respeten las normas de privacidad, cada contrato incluye cláusulas específicas que obligan a los terceros a proteger los datos con el mismo rigor que nosotros. Además, realizamos auditorías y revisiones periódicas para garantizar el cumplimiento de estas normas. Toda la información compartida se maneja a través de nuestro departamento legal, que supervisa la redacción y ejecución de estos contratos.

Pregunta #6 ¿Qué procedimientos tiene la empresa en caso de violaciones de datos o brechas de seguridad?

En caso de violaciones de datos o brechas de seguridad, nuestra empresa sigue un protocolo bien definido para abordar el problema de manera rápida y eficiente. Primero, se elabora un

informe detallado sobre la naturaleza de la violación y el alcance de los datos comprometidos. Este informe se realiza con celeridad para minimizar el impacto.

Las sanciones para los empleados involucrados en una brecha de seguridad pueden variar desde amonestaciones hasta el despido, dependiendo de la gravedad del incidente. Si se determina que hubo una violación significativa y un perjuicio económico, la empresa puede tomar acciones legales contra los responsables.

Además, nuestro sistema de seguridad incluye monitoreo constante y detección de intrusos en tiempo real. Si se detecta una actividad sospechosa, se activa una alarma y se notifica al equipo de seguridad para que tomen medidas inmediatas. La empresa también realiza evaluaciones periódicas de riesgo para mejorar continuamente nuestras defensas contra posibles amenazas.

Pregunta #7 ¿La empresa realiza evaluaciones periódicas de riesgos de privacidad? En caso afirmativo, ¿cómo se llevan a cabo?

Sí, nuestra empresa realiza evaluaciones periódicas de riesgos de privacidad para proteger los datos sensibles de los usuarios. Estas evaluaciones se llevan a cabo mediante un sistema integral que incluye varias capas de seguridad y procesos específicos para identificar y mitigar amenazas. Implementamos un monitoreo constante en todas las unidades, segmentando y delimitando la información para asegurar que solo el personal autorizado acceda a los datos necesarios. Utilizamos herramientas avanzadas de detección y prevención de intrusiones (IDS y IPS) que nos alertan en tiempo real sobre cualquier actividad sospechosa.

Ante una alerta, nuestro equipo de seguridad toma medidas inmediatas para mitigar la amenaza. Realizamos evaluaciones iniciales y periódicas para identificar vulnerabilidades y determinar las acciones correctivas necesarias. Este enfoque nos permite mejorar continuamente nuestras defensas y actualizar nuestras políticas de privacidad y seguridad. También utilizamos aplicaciones que nos envían alertas por correo electrónico si detectan interferencias o actividades sospechosas en nuestro sistema informático.

Análisis.

De la experiencia recopilada, se analiza que si se tiene conocimientos de las posibles responsabilidades se trabaja de forma idónea, las empresas para las que trabaja tienen

estándares muy elevados de calidad para el tratamiento de la información, desde la recolección hasta la transferencia de los datos, mecanismos de seguridad para protegerlo y la posibilidad de revocar los mismos, ya que se firma un contrato, donde la exigencia principal es que el usuario o titular de los datos conozca a certeza el fin del uso que tendrán, no obstante esto no sucedía hace 3 años donde se vieron en la necesidad de exigir la firma de los usuarios para los contratos de entrega de datos, lo que coincide con la existencia de la nueva normativa europea en relación a la protección de datos personales y el desarrollo masivo de la inteligencias artificiales. De lo que se puede analizar, es que no dependen del estado para exigir el cumplimiento de las normativas ya que ellos se basan en reglamento europeo y normativas ISO que les establece cual es la ruta más idónea del manejo de datos, la carencia de coerción les faculta a decidir si ser probos o utilizar los datos con fines exentos a los permitidos por la ley o mucho peor obtener tus datos sin el consentimiento. Esta exigencia se vuelve más alarmante porque nos expresa que ya se está utilizando la IA para el potenciamiento de servicios, donde nos convertimos en datos para una red neuronal que venderá más eficiente en tanto y cuanto sepa de nosotros.

2.1.6 Análisis de Entrevista dirigida a ciudadana

Nombre del entrevistado: Brenda Reyes Tomalá

Fecha de la entrevista: Miércoles, 29 de mayo de 2024

Lugar de la entrevista: Universidad Estatal península de Santa Elena

Pregunta #1: ¿Podría compartir con nosotros su experiencia específica con la obtención y uso ilegítimo de sus datos sensibles?

Ocurre que llega a mi correo personal una factura que había sido expedida por Claro, donde se me notificaba sobre la compra de una línea telefónica, que yo no había solicitado. De hecho, no había ninguna relación contractual con ellos. Con esta notificación que me acerqué a servicios al cliente para pedir explicación, revisaron los registros me encuentro que esa no había sido la única línea, sino que, había 7 u 8 líneas telefónicas, que habían sido adquiridas entre diciembre del 2023 y febrero del 2024. Lo cual generó una alarma en mí, dadas las circunstancias y las condiciones en las que está nuestro país en el ámbito delictivo, pues generalmente estas líneas son usadas para extorsiones u otro tipo de actos delictivos, yo necesitaba las explicaciones de por qué la operadora había generado una situación contractual en ausencia de mi consentimiento. Entonces ellos me hicieron conocer que

bastaba con mi cédula, el numero o la copia, se podía hacer esa compra, quise profundizar, porque los números de cédula de las personas son de conocimiento público en este momento, nosotros ponemos en el internet. Es allí donde se generó mi preocupación, puesto que puedo deducir que estoy en el escenario en el que mis datos personales han sido utilizados de forma fraudulenta para la adquisición de estas líneas telefónicas y establecer compromisos, procedí inmediatamente a cancelar esos servicios con la declaración de que mi manifestación expresa de voluntad no fue requerida para estos contratos.

Pregunta #2: ¿Conoce cómo se produjo la violación de la seguridad de sus datos sensibles? No, realmente no me dieron ninguna explicación que satisfaga mis consultas, ellos refirieron que bastaba con la cédula nada más para poder hacer eso, lo cual me parece un poco absurdo porque si estoy en sus registros, si consto como usuaria, definitivamente pues ellos deberían ratificar que esa manifestación de la voluntad sea legítima, lo cual no se había hecho.

Pregunta #3: ¿Cuáles fueron las principales consecuencias que enfrentó como resultado del uso ilegitimo de sus datos?

Yo no podría referir consecuencias, quise evitar las consecuencias actuando de manera rápida ante lo ocurrido, pero sí puedo referir que entre las ocho líneas telefónicas que me fueron atribuidas, yo encontré en mi registro de llamadas, tal vez tres llamadas de uno de esos números que habían sido expedidos a mi número. me parece un poco curioso, que compran a mi nombre y tienen acceso a mi número celular, pero referir consecuencias no hasta ese momento, más bien quise prevenirla reaccionando oportunamente.

Pregunta #4: ¿Ha recibido alguna compensación o reparación por los daños sufridos como resultado del uso ilegítimo de sus datos sensibles?

No, ninguna, absolutamente ninguna. De hecho, el trámite representó para mí 48 horas después de haber metido el papel en la agencia de la compañía. Recibí un compromiso verbal que no tiene realmente para mí ningún valor, el hecho que me dijeron que cada vez que yo quiera abrir una nueva cuenta con ellos, comprar una línea, esto va a ser sujeto a revisiones, pero realmente eso fue un discurso para evadir lo que representaba el hecho de haber establecido relaciones de intercambio, en este caso de servicio, a partir solo de una copia, porque asumo que quien hizo estas compras solo referenció mi número, dado que la manifestación expresa de la voluntad no fue verificada.

Pregunta #5: ¿Cómo describiría su nivel de confianza en las empresas y organizaciones que manejan y almacenan datos sensibles después de lo sucedido?

Es totalmente negligente, deficiente, porque el solo hecho que sus propios trabajadores se tomen la libertad de hacernos llamadas a los usuarios en cualquier hora, a cualquier momento, a ofrecer servicios, ya es una violación en el uso de esta información, porque debería establecerse si los usuarios queremos recibir vía telefónica o no ofertas de servicios por parte de quienes son poseedores de este tipo de información, de nuestros datos. No tanto en cómo almacenan la información, sino en cómo sus procedimientos internos para generar, en este caso, prestación de servicios, usan nuestra información para sacar beneficios. Nuestros números de teléfono están a disposición de ellos, ellos los usan para posicionar su marca o servicio, y pues, lo que para mí fue un requisito para tener una línea telefónica, mi cédula, mi número de teléfono, mi dirección, para ello se vuelve una oportunidad de negocio, de vender sus productos. Entonces desde esa perspectiva debería ser, ¿está usted de acuerdo que operadores de nuestro servicio o empleados de nuestra empresa le contacten para ofrecer nuevos servicios? Si quiero o no quiero.

Pregunta #6: ¿Cree que hay aspectos específicos de la regulación de protección de datos que podrían mejorarse para prevenir casos como el suyo en el futuro?

No he leído a profundidad las regulaciones, pero sí creo que se les escapa mucho de lo que conozco, aspectos vinculados al manejo tecnológico. El problema es que ese custodio de datos personales, de datos sensibles, hace uso de las tecnologías para hacer uso ilegitimo de esa información. Y creo que, las vulnerabilidades de esta tecnología, es en lo que hay que trabajar y el compromiso. Yo creo que los alcances y límites para los custodios de nuestros datos personales no son lo suficientemente claros, es un tema de comportamiento ético, también de manejo ético de estas entidades. No creo que la solución sería una nueva, un nuevo organismo, entidad gubernamental, creo que los actores del proceso deben hacer lo que deben de hacer y si no lo hacen, pues las normas deberían reprimir esos comportamientos de manera severa.

Pregunta #7 ¿Sabía usted a qué autoridad acudir para dar a conocer este uso ilegítimo de los datos sensibles?

Hay tipos penales que consignan este tipo de uso ilegítimo, de hecho, no judicialicé el caso, sí estaba tentada a denunciar, porque me generaba mucha incertidumbre el hecho de que usen esas líneas para hechos delictivos, y verme envuelta en situaciones de esa naturaleza. Eso me motivaba a judicializarlo, Ya luego cuando, con el requerimiento que hice a la compañía y la aceptación que ellos dieron, tengo los documentos que dejan claramente establecido que yo no di consentimiento para apertura esas líneas.

No se me ocurrió acudir a la Defensoría del Pueblo, porque realmente, no me considero consumidora, debido a que no soy usuaria de ellos. Yo no reclamaba la prestación del servicio de ellos, reclamaba el mal uso de mis datos personales, debido a que posiblemente la fuente pudo haber sido otra, no ellos propiamente. Lo que yo cuestionaba eran los procedimientos que ellos siguen para generar líneas telefónicas a mi favor y realmente no, no pensé que la Defensoría del Pueblo pueda asistirme en esto, el estado tiene el deber de hacer cumplir la normativa, sin que necesariamente se creen nuevas entidades para el control.

Análisis.

Los hechos facticos presentados por la ciudadana Brenda Reyes nos permiten comprender como la abrumante era digital nos ha rebasado, las mismas actuaciones del pasado se sostienen hasta el presente en industrias como las telefónicas, la facilidad con la que un tercero puede tener acceso a nuestros datos sensibles como los de identidad, es aterrador, los hechos expuestos nos llevaron analizar los siguiente; Los datos sueltos por la internet o que son transferidos sin el consentimiento en su conjunto configuran el mosaico de la identidad del sujeto y con este trabajo hecho se generarían afectaciones que a nuestra percepción no nos parecerían graves, sin embargo primero pueden ser 7 líneas telefónicas distintas con el posible objetivo de extorsiona, ocultando al verdadero propietario de las mismas, luego sería la compra de servicios más cuantiosos y quizás estos datos individuales flotando por la internet debido al negligente tratamiento servirán para construir la identidad digital de Brenda Reyes para poder tener un perfil a quien venderle productos o servicios o mucho peor, se podría afectar su imagen y reputación con inteligencia artificial vulnerando así el derecho al buen nombre, todo esto sin contar con el consentimiento informado y expreso del titular de los datos.

Los elementos del consentimiento como los establece el artículo 8 de la LOPDP no se encuentran aplicados en el presente caso, no existe libertad ya que no es la voluntad de la

señora Brenda entregar los datos, no es especifica porque no hay información en relación a los fines, mucho menos informada pues nunca fue comunicada de forma efectiva y transparente y en definitiva no es inequívoco el consentimiento ya que ni si quiera sabia de la existencia de esta relación comercial electrónica, no es posible la existencia de un consentimiento tácito o suspensivo porque no hay manifiesta voluntad, lo inseguro es que dicha telefónica no tiene mecanismos que garanticen seguridad y transparencia para sus usuarios presentando un gran problemática para la sociedad ecuatoriana que sufre una gran ola de inseguridad y extorsión que se suele ejecutar a través de llamadas telefónicas, lo que origina un reto para el estado hacer cumplir sus reglas puesto que no se observa la rigurosidad del mismo en este caso.

La facultad que tienen las empresas debido a la falta de coerción por parte del estado para hacer cumplir las disposiciones normativas que pese a no ser lo suficientemente rigurosas, han vulnerado el derecho a la protección de datos en el presente caso, porque no ha existido el cumplimiento de los elementos del consentimiento y eso es un hecho factico, dejando claro que esta no es la regla general que aplican las entidades privadas, este es un caso de tantos donde no cumple con lo establecido en el artículo 66 numeral 11 y 19 de la constitución de la república del Ecuador, ya que se establece claramente la prohibición del uso sin la autorización del titular de los datos y por corolario lógico se garantiza el derecho a la protección de datos.

4.2 Verificación de la idea a defender

En relación con el presente trabajo de investigación y los datos adquiridos a través de encuestas, entrevistas y una amplia investigación bibliográfica, se verifica la idea a defender: "La falta de reglas respecto a los elementos del consentimiento en el uso de datos sensibles establecidos en el artículo 8 de la ley orgánica de protección de datos personales faculta a las empresas del ámbito privado a vulnerar el derecho a la protección de datos".

Por tanto, se establece que existe una falta de disposiciones normativas que desarrollen los aspectos relevantes dentro de los elementos establecidos en el consentimiento, legislado por la ley orgánica de protección de datos personales, en relación al consentimiento libre como el caso de los menores de edad que son incapaces relativos, especifica, informada e inequívoca ya que no se presentan las garantías para que los usuarios tengan seguridad del uso que se tendrá de los datos sensibles, de cómo se trataran o si se transferirán. Los jueces de primer nivel han manifestado que el problema existente en el consentimiento al momento de firmar un contrato radica en la falta de información proporcionada por las entidades privadas, ya que suelen ser muy complejas y las personas firmantes no entienden completamente lo que están autorizando, parte de la responsabilidad también recae en los ciudadanos, quienes no leen para su propio beneficio.

Además, se ha observado que las entidades privadas mencionan el tratamiento y uso de datos, pero a menudo se refieren a los datos de sus trabajadores, y las grandes corporaciones si contemplan por principios de calidad el consentimiento en el uso de los datos de sus clientes.

Esta laguna en la regulación y la supervisión permiten a las empresas ilegalmente operar el tratamiento de datos, exponiendo a los usuarios a riesgos de vulneración de privacidad. La falta de claridad y de normas estrictas en la legislación actual, específicamente las relacionadas a los elementos del consentimiento, permite a las empresas privadas manejar datos sensibles sin una adecuada rendición de cuentas. Esta práctica confirma que la falta de control del estado en las empresas privadas junto a que no se tenga regulada la gestión de la información y los datos sensibles que recogen de sus usuarios, se presenta en una grave vulneración al derecho a la protección de datos, establecido en el art 66 numeral 19.

CONCLUSIONES

Después de completar el proceso investigativo integral que implicó el presente trabajo, en el cual incluyó la revisión de una amplia literatura relacionada con las variables en cuestión y la recolección de información a través de entrevistas y encuestas dirigidas a jueces, entidades privadas y personas naturales, se ha llegado a varias conclusiones:

Primero, se ha evidenciado una inaplicación significativa de la LOPDP, debido a que las entidades privadas, en muchas ocasiones, carecen de un protocolo o reglamento interno que les oriente sobre cómo abordar un conflicto en caso de una fuga de información. Debido a que el estado no les obliga a cumplir la expresa normativa y la falta de procedimientos claros produce violaciones a la protección de datos y a una respuesta inadecuada ante situaciones de riesgo.

Segundo, se ha constatado, que debido a la responsabilidad adquirida entre las partes al suscribir el contrato para la cesión de los datos sensibles, es trascendental, que el usuario se asegure de leer detenidamente y comprender las cláusulas del contrato, garantizando que no sean desproporcionales entre el servicio que se recibe y el uso de los datos sensibles. Al mismo tiempo, las entidades privadas tienen la responsabilidad de redactar los contratos de manera clara, sencilla y concreta para garantizar la seguridad del usuario y evitar malentendidos.

Tercero, que los contratos de adhesión se presentan como un elemento adicional a nuestra problemática de la investigación, especialmente cuando son elaborados por empresas extranjeras. Esto se debe, a que la jurisdicción extraterritorial complica considerablemente el proceso judicial, lo que puede obstaculizar la protección efectiva de los derechos del usuario y dilatar la resolución de conflictos.

Cuarto, según los principios de libre mercado, ofrecer un buen servicio requiere que las empresas privadas mantengan estándares de calidad eficientes y eficaces. Esto no solo garantiza a los usuarios la certeza de que pueden confiar en la empresa con su información, sino que también obliga a las empresas a establecer protocolos robustos para el manejo de datos sensibles. Estos protocolos son implementados voluntariamente por las empresas, no por coerción estatal.

RECOMENDACIONES.

- Es fundamental implementar una supervisión rigurosa por parte de las autoridades competentes en relación con el manejo adecuado de los datos sensibles de los usuarios por parte de las empresas privadas. Esta medida mejoraría la confianza del titular en la protección de su privacidad y fomentaría que los negocios sean cada vez más éticos y transparentes.
- Además de esta supervisión, es perentorio que las autoridades sancionen rigurosamente a las entidades privadas que incumplan con las normas establecidas. Al mismo tiempo, es necesario que las personas se eduquen individualmente sobre temas como la comprensión de los términos y condiciones de los contratos. Una mayor educación en este aspecto permitirá a los ciudadanos tomar decisiones informadas y proteger mejor sus propios intereses.
- En el contexto internacional, los contratos pueden plantear problemas debido a la diferencia de jurisdicciones. Por ello, abogar por la armonización de las leyes de protección de datos a nivel internacional es fundamental. Esta armonización facilitaría la cooperación entre países y la resolución de conflictos transfronterizos, brindando una mayor protección a los usuarios y una mayor claridad legal a las empresas que operan a nivel global. De esta forma, se promovería la igualdad de condiciones para todas las partes involucradas, asegurando que los derechos de los usuarios sean respetados sin importar la jurisdicción en la que se encuentren.
- Por último, el estado, a través de los órganos encargados debe ser garante del cumplimiento del derecho a la protección de datos, estableciendo mecanismos para obligar a las entidades privadas a mantener un orden y estándares de calidad y protección en el manejo de los datos.

BIBLIOGRAFÍA

1. American Psychological Association. (2019). *NORMAS APA 7MA EDICIÓN.*
2. Asamble Nacional. (2002). *Ley de Comercio Electrónico, firmas y mensajes de datos.* Quito.
3. Asamblea General de las Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos* . Paris.
4. Asamblea Nacional. (2000). *LEY ORGÁNICA DE DEFENSA DEL CONSUMIDOR.* QUITO.
5. Asamblea Nacional. (2008). CONSTITUCIÓN. En A. NACIONAL, *HABEAS DATA.* QUITO.
6. Asamblea Nacional. (2021). *Ley Orgánica de Protección de Datos Personales.* QUITO.
7. ASAMBLEA NACIONAL. (2023). *REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES.*
8. ASOCIACIÓN DE ACADEMIAS DE LENGUAS ESPAÑOLAS. (2023). *Diccionario Prehispánico del Español Jurídico*. Obtenido de https://dpej.rae.es/lema/dato-sensible
9. Barturén, T. (2011). EL CONTROL DE LAS CLAUSULAS ABUSIVAS EN EL CODIGO DE PROTECCION Y DEFENSA DEL CONSUMIDOR. *Revista de Investigación Jurídica*. Obtenido de https://elibro.net/es/ereader/upse/27970?page=2.
10. Cabanellas, G. (1979). *Diccionario juridico elemental.*
11. Castro Cruzatt, Karin. (2008). El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú. *IUS ET VERITAS: Revista de la Asociación IUS ET VERITAS, 18*(37), 260-276.
12. Diccionario de la Real Academia Española de la Lengua. (s.f.). *Diccionario de la Real Academia Española de la Lengua.*
13. Fayos Gardó, Antonio. (2015). *Los derechos a la intimidad y a la privacidad en el siglo XXI.* Librería-Editorial Dykinson.
14. Foro económico mundial. (2023). *The Global Risks.* Switzerland. Obtenido de https://www.weforum.org/reports/global-risks-report-2023/
15. Gamboa, C. (2007). DERECHO DE LA INTIMIDAD Y EL HONOR VS. DERECHO A LA INFORMACIÓN. En *Estudio Teórico Conceptual, Marco Jurídico a Nivel Federal y Estatal e Iniciativas presentadas en la materia en la LIX Legislatura.*

16. Garcia Falconi, J. C. (2000). *Manual de práctica procesal constitucional. El juicio especial por la acción de hábeas data y los derechos constitucionales a la intimidad, privacidad, imagen al honor a la no discriminación a la igualdad al de petición al de información sus limitaciones* . Quito: Ediciones Rodín.

17. Garcia Falconí, José. (2000). *El juicio especial de habeas data; y los derechos constitucionales a: la intimidad; privacidad; imagen; al honor; a la no discriminación; a la igualdad; al de petición; al de información, sus limitaciones y responsabilidades.* Rodin. Obtenido de biblioteca UPSE

18. Garriga Dominguez, A. (s.f.). *Nuevos retos para la protección de datos personales en la era del Big Data y de la computación ubicua.* Obtenido de https://elibro.net/es/ereader/upse/58235?page=5

19. Martí de Gidi, Luz. (2018). *Vida privada, honor, intimidad y propia imagen como derecho humanos.*

20. ONU, A. G. (1966). *PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS.*

21. Oro Badia, Ramon. (s.f.). *La protección de datos.* Editorial UOC.

22. Pfeiffer, María Luisa. (enero-junio de 2008). Derecho a la privacidad. Protección de los datos sensibles. *Revista Colombiana de Bioética, 3*(1), 11-36.

23. Randy E Barnett. (2004). Una teoría del consentimiento contractual. *Revista de serecho THEMIS*(49). Obtenido de http://revistas.pucp.edu.pe/index.php/themis/article/view/8568/8925

24. Rebollo Delgado, L. (2008). *Introducción a la protección de datos* (2a ed ed.). Obtenido de https://elibro.net/es/lc/upse/titulos/63115

25. Rebollo Delgado, L., & Mercedes Serrano, M. (2008). *INTRODUCCIÓN A LA PROTECCIÓN DE DATOS* (Segunda ed.). Madrid: Dykinson. Recuperado el 2023, de https://elibro.net/es/ereader/upse/63115?page=6

26. Rebollo, D. (2018). *Introducción a la protección de datos: (2 ed.).* Madrid: Dikinson. Obtenido de https://elibro.net/es/ereader/upse/63115?page=38.

27. Rebollo, L. (2010). *Introducción a la protección de datos.* Dykinson, S.L.

28. REYES, BRENDA; CASTILLO, CARLOS. (2015). *GUIA METODOLOGICA PARA PROYECTOS DE INVESTIGACIÓN SOCIAL.* SANTA ELENA.

29. Sabater, Carmen. (2018). VIDAS DE CRISTAL: ANÁLISIS DEL DERECHO A LA INTIMIDAD EN LA SOCIEDAD DE LA INFORMACION. *Intersticios Revista sociológica de pensamiento crítico, 2*(1), 43-54. Obtenido de http://www.intersticios.es

30. The Council of Europe. (1981). *CONVENIO PARA LA PROTECCION DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS*

DE CARACTER PERSONAL. Obtenido de STE 108 – Tratamiento automatizado de datos de caracter personal, 28.I.1981

31. Union Europea. (1995). *Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.* Strasburgo: Parlamento Europeo. Obtenido de https://www.boe.es/doue/1998/024/L00001-00008.pdf

32. Union Europea. (1998). *Directiva 97/66/CE.* Estrasburgo: Parlamento Europeo. Obtenido de https://www.boe.es/doue/1995/281/L00031-00050.pdf

33. Vergara Rojas, Manuel. (2017). *Chile: Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales* (Vol. 6). doi:https://dx.doi.org/10.5354/0719-2584.2017.45822

34. WESTIN, A. (1972). *Data banks in a free society.* New York: Quadrangle.

ANEXOS

GRÁFICO 13 ENTREVISTA A JUEZ
Entrevista a Juez Juan Camacho.

Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Entrevista realizada a jueces

GRÁFICO 14 ENTREVISTA A JUEZ
Entrevista a Juez Richard Gavilanes.

Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Entrevista realizada a jueces

GRÁFICO 15 ENTREVISTA A JUEZ

Entrevista a Juez de Ana Tapia

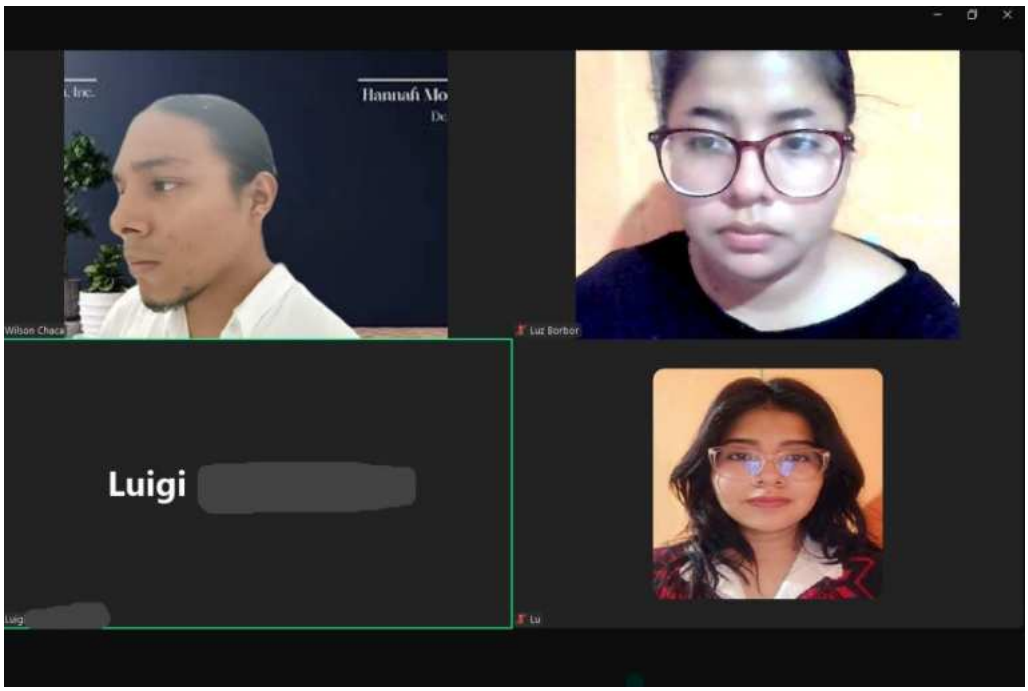
Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Entrevista realizada a jueces

GRÁFICO 16 ENTREVISTA A ENTIDAD PRIVADA

Entrevista a Entidad privada “Disnacon”

Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Entrevista realizada a entidad privada.

GRÁFICO 17 ENTREVISTA A ENTIDAD PRIVADA
Entrevista a Entidad privada en anonimato.



Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Entrevista realizada a entidad privada.

GRÁFICO 18 A CIUDADANA
Entrevista a ciudadana

Elaborado por: Luz Borbor y Wilson Chaca – Fuente: Entrevista realizada a ciudadana.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

CARRERA DE DERECHO

TRABAJO DE INTEGRACION CURRICULAR: CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023

INVESTIGADORES: LUZ PATRICIA BORBOR SUÁREZ Y WILSON JAILMAR CHACA BRAVO

ANEXO 1 CARTA DE CONSENTIMIENTO

PROPÓSITO

Primero: El propósito de este documento es obtener su consentimiento para recolectar información personal de las entrevistas que se llevarán a cabo en el lugar que usted disponga.

Segundo: Así también se busca analizar la información obtenida de las entrevistas con motivos de estudio, que son de suma importancia para el TRABAJO DE INTEGRACIÓN CURRICULAR: CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023.

Tercero: Los datos serán de uso único y exclusivo para análisis e investigación del CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023.

Cuarto: La información revelada no será utilizada para ser publicada en ningún medio u otro propósito.

Quinto: Si está conforme con el propósito de investigación proceda a firmar el documento.

CONSENTIMIENTO: Yo, el interesado, doy permiso de usar la información obtenida durante las sesiones de entrevista con fines de estudio ya mencionados.

NOMBRE: _____

FECHA: _____

CI:_____

ENTREVISTADORES: Luz Patricia Borbor Suárez y Wilson Jailmar Chaca Bravo

FIRMA

Agradecemos vuestra colaboración

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

CARRERA DE DERECHO

TRABAJO DE INTEGRACION CURRICULAR: CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023

INVESTIGADORES: LUZ PATRICIA BORBOR SUÁREZ Y WILSON JAILMAR CHACA BRAVO

ANEXO 2 CUESTIONARIO APLICADO A CIUDADANOS

OBJETIVO: Evaluar el nivel de conciencia y preocupación de la población respecto a la protección y manejo de datos sensibles, así como su percepción sobre la efectividad de las medidas de seguridad implementadas por las organizaciones que recopilan y utilizan dicha información.

Estimado Usuario: Sírvase dar lectura al presente cuestionario que permitirá profundizar aspectos relevantes en esta investigación, recomendamos dar respuesta con una X según corresponda.

1. ¿Conoce usted cuáles son sus datos/información sensible?

   SI ☐ NO ☐

2. ¿Conoce usted que toda empresa que obtiene datos sensibles de sus clientes debe declarar los términos y condiciones de su uso?

   SI ☐ NO ☐

3. ¿Cuándo usted cede a la compra de un bien o servicio y entrega datos personales es requerido su consentimiento?

   SIEMPRE ☐ NUNCA ☐ A VECES ☐

4. ¿Lee usted los términos y condiciones cuando las entidades o plataformas le piden su consentimiento?

   SI ☐ NO ☐ A VECES ☐

5. ¿Te resultan claros los términos y condiciones sobre la protección de datos?

   LA MAYORÍA DEL TIEMPO ☐ EN LO ABSOLUTO ☐

6. ¿Sabías que si tus datos sensibles se utilizan para otro propósito sin tu autorización, se estarían vulnerando tus derechos a la protección de datos?:

   POR SUPUESTO ☐ NO SABÍA ☐

7. ¿Sabía usted que tiene el derecho a revocar el consentimiento de uso de datos personales por parte de empresas privadas?

   SI ☐ NO ☐

8. Sabe usted si sus datos personales o el de alguno de sus conocidos han sido utilizados con otros propósitos por parte de empresas a las que se les entregó sus datos

   SI ☐ NO ☐

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
CARRERA DE DERECHO
TRABAJO DE INTEGRACION CURRICULAR: CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023

INVESTIGADORES: LUZ PATRICIA BORBOR SUÁREZ Y WILSON JAILMAR CHACA BRAVO

ANEXO 3 ENTREVISTA A JUECES DE PRIMER NIVEL

ENTREVISTA A JUECES DE PRIMER NIVEL DE LA PROVINCIA DE SANTA ELENA

OBJETIVO: Valorar la opinión de los jueces de garantías jurisdiccionales de consejo de la judicatura de la provincia de Santa Elena en relación con el consentimiento de los datos sensibles y las vías efectivas para ejercitar el derecho a la acción.

Estimado Juez/a: Sírvase dar lectura al presente cuestionario que permitirá profundizar aspectos relevantes en esta investigación.

1. ¿Cuáles son los principales problemas de la relación que existe entre el derecho a la protección de datos y el consentimiento al entregar los datos sensibles?
2. ¿Considera que la falta de desarrollo de los elementos del consentimiento establecidos en el artículo 8 de la Ley Orgánica de protección de datos vulnera el derecho a la protección de datos?
3. ¿Según su experiencia cuál considera son los procedimientos más eficaces para que los ciudadanos puedan acceder a la actualización, rectificación, eliminación o anulación de los datos sensibles? Previo a ejercer el habeas data
4. ¿En el ejercicio de su profesión cuales han sido los casos más relevantes que ha manejado en torno a las vulneraciones al consentimiento en el uso de los datos personales?
5. Sabiendo que los datos en la era digital se han convertido en los activos más valiosos de las empresas privadas, ¿Cómo se establecería la reparación integral si la entidad privada se niega a dejar de usar y almacenar, luego de que se haya solicitado por la vía de comunicación idónea la revocatoria del consentimiento?

Agradecemos vuestra colaboración

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
CARRERA DE DERECHO
TRABAJO DE INTEGRACION CURRICULAR: CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023

INVESTIGADORES: LUZ PATRICIA BORBOR SUÁREZ Y WILSON JAILMAR CHACA BRAVO

ANEXO 4 ENTREVISTA A FUNCIONARIO

ENTREVISTA A FUNCIONARIO DE LA DINARP

OBJETIVO: Obtener información detallada sobre los procesos y procedimientos utilizados por la Dirección Nacional de Registros Públicos para la gestión y custodia de registros públicos, así como para comprender su enfoque en la protección de datos sensibles y la garantía de la transparencia y acceso a la información para los ciudadanos

Estimado funcionario: Sírvase dar lectura al presente cuestionario que permitirá profundizar aspectos relevantes en esta investigación.

1. ¿Qué mecanismos del estado existen para garantizar que los titulares de datos estén informados sobre las finalidades del tratamiento de sus datos?
2. ¿Cuáles son las implicaciones del principio de consentimiento informado en situaciones donde los datos personales se recopilan a través de dispositivos de IoT (Internet de las cosas) y otros dispositivos conectados, donde el consentimiento puede no ser directamente otorgado por los usuarios?
3. ¿Cuáles son los procedimientos establecidos para garantizar la seguridad y privacidad de los datos sensibles de las personas? ¿Qué medidas toman en caso de que se produzca una vulneración de datos?
4. ¿Cuál es la estructura organizativa de su entidad en relación con la protección de datos sensibles? ¿Cómo se dividen en departamentos o áreas y cuál es el papel de cada una en asegurar la seguridad y privacidad de esta información?
5. ¿Podrían compartir ejemplos específicos de cómo han abordado tales situaciones en el pasado?

Agradecemos vuestra colaboración

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
CARRERA DE DERECHO
TRABAJO DE INTEGRACION CURRICULAR: CONSENTIMIENTO EN EL USO DE DATOS SENSIBLES Y LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO PRIVADO, 2023

INVESTIGADORES: LUZ PATRICIA BORBOR SUÁREZ Y WILSON JAILMAR CHACA BRAVO

ANEXO 5 ENTREVISTA A CIUDADANA

ENTREVISTA A CIUDADANA

OBJETIVO: Entrevistar a una ciudadana afectada por el robo de identidad y el uso fraudulento de sus datos sensibles es importante para comprender el consentimiento en el manejo de estos datos por empresas privadas. Su testimonio ofrece una visión concreta de los riesgos y consecuencias y señala deficiencias en la protección de datos.

Estimada ciudadana: Sírvase dar lectura al presente cuestionario que permitirá profundizar aspectos relevantes en esta investigación.

1. ¿Podría compartir con nosotros su experiencia específica con la obtención y uso ilegítimo de sus datos sensibles?
2. ¿Conoce cómo se produjo la violación de la seguridad de sus datos sensibles?
3. ¿Cuáles fueron las principales consecuencias que enfrentó como resultado del uso ilegitimo de sus datos?
4. ¿Ha recibido alguna compensación o reparación por los daños sufridos como resultado del uso ilegítimo de sus datos sensibles?
5. ¿Cómo describiría su nivel de confianza en las empresas y organizaciones que manejan y almacenan datos sensibles después de lo sucedido?
6. ¿Cree que hay aspectos específicos de la regulación de protección de datos que podrían mejorarse para prevenir casos como el suyo en el futuro?
7. ¿Sabía usted a qué autoridad acudir para dar a conocer este uso ilegítimo de los datos sensibles?

Agradecemos vuestra colaboración

INVESTIGADORES: LUZ PATRICIA BORBOR SUÁREZ Y WILSON JAILMAR CHACA BRAVO

ANEXO 6 ENTREVISTA A ENTIDAD PRIVADA

ENTREVISTA A ENTIDAD PRIVADA

OBJETIVO: Obtener una comprensión profunda y detallada de las políticas, prácticas y desafíos relacionados con el tratamiento de datos sensibles en la empresa telefónica, explorando cómo la empresa recolecta, almacena, procesa y protege los datos sensibles de sus clientes, así como comprender las medidas y controles implementados para garantizar la seguridad y privacidad de estos datos.

Estimado ciudadano: Sírvase dar lectura al presente cuestionario que permitirá profundizar aspectos relevantes en esta investigación.

1. ¿Cuáles son los tipos de datos sensibles que su empresa recopila de los usuarios?
2. ¿Cómo obtiene la empresa el consentimiento de los usuarios para utilizar sus datos sensibles?
3. ¿Qué políticas tiene la empresa en relación con el consentimiento y el uso de datos sensibles?
4. ¿Cómo se almacenan y protegen los datos sensibles de los usuarios?
5. ¿La empresa comparte los datos sensibles de los usuarios con terceros? En caso afirmativo, ¿cómo se aseguran de que se respeten las normas de privacidad?
6. ¿Qué procedimientos tiene la empresa en caso de violaciones de datos o brechas de seguridad?
7. ¿La empresa realiza evaluaciones periódicas de riesgos de privacidad? En caso afirmativo, ¿cómo se llevan a cabo?

Agradecemos vuestra colaboración