



**UNIVERSIDAD ESTATAL  
PENÍNSULA DE SANTA ELENA**

**FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD CARRERA  
DE DERECHO**

**TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA  
OBTENCIÓN DEL TÍTULO DE ABOGADA**

**TÍTULO:  
ESTUDIO COMPARADO A LAS REGLAS DEL HABEAS DATA DE  
LAS LEGISLACIONES DE ECUADOR, ARGENTINA Y PERÚ 2024**

**AUTORA:  
KATHERINE ESTEFANIA CORNEJO PONCE**

**TUTOR:  
AB. PEDRO ALVAREZ BETANCOURT, MGT.**

**LA LIBERTAD – ECUADOR  
2024**

**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA**

**FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD CARRERA  
DE DERECHO**

**TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA  
OBTENCIÓN DEL TÍTULO DE ABOGADA**

**TÍTULO:  
ESTUDIO COMPARADO A LAS REGLAS DEL HABEAS DATA DE  
LAS LEGISLACIONES DE ECUADOR, ARGENTINA Y PERÚ 2024**

**AUTORA:  
KATHERINE ESTEFANIA CORNEJO PONCE**

**TUTOR:**

**AB. PEDRO ALVAREZ BETANCOURT, MGT.**

**LA LIBERTAD – ECUADOR  
2024**

## **APROBACIÓN DEL TUTOR**

### **CERTIFICO**

Que he analizado el trabajo de integración curricular con el título **“ESTUDIO COMPARADO A LAS REGLAS DEL HABEAS DATA DE LAS LEGISLACIONES ECUADOR, ARGENTINA Y PERÚ 2024”** presentado por la estudiante KATHERINE ESTEFANIA CORNEJO PONCE, portadora de la cédula de ciudadanía N° 240018724-7 respectivamente, como requisito previo a obtener el título de ABOGADA, 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.



AB. PEDRO XAVIER ALVAREZ BETANCOURT, MGT

**TUTOR**

## **CERTIFICACIÓN ANTIPLAGIO**

### **CERTIFICO**

En mi calidad de Tutor del Trabajo de Integración Curricular: **“ESTUDIO COMPARADO A LAS REGLAS DEL HABEAS DATA DE LAS LEGISLACIONES ECUADOR, ARGENTINA Y PERÚ 2024”**, perteneciente a KATHERINE ESTEFANIA CORNEJO PONCE estudiante de la Carrera de Derecho, CERTIFICO, que el contenido de dicho trabajo ha sido sometido a la validación en sistema antiplagio COMPILATIO, obteniendo un porcentaje de similitud del 8%, cumpliendo así con los parámetros técnicos requeridos para este tipo de trabajos académicos.



AB. PEDRO XAVIER ALVAREZ BETANCOURT, MGT.  
**TUTOR**

## **VALIDACIÓN GRAMATICAL Y ORTOGRÁFICA**

### **CERTIFICO**

Que, he revisado el trabajo de Integración Curricular de título: **“ESTUDIO COMPARADO A LAS REGLAS DEL HABEAS DATA DE LAS LEGISLACIONES ECUADOR, ARGENTINA Y PERÚ 2024”**, elaborado por la estudiante de la Carrera de Derecho de la Universidad Estatal Península de Santa Elena: **KATHERINE ESTEFANIA CORNEJO PONCE**, previo a la obtención del título de abogada.

Que, he realizado las observaciones pertinentes en los ámbitos de la gramática, ortografía y puntuación del documento, misma que han sido acogidas proactivamente por la mencionada señorita, corroborando así, que han sido introducidos los ajustes correspondientes en el trabajo en mención.

por lo expuesto, autorizo a las peticionarias, hacer uso de este certificado como a bien convengan.



**Lcda. KERLY VANESSA RAMOS RAMOS**  
**Magister en Lengua Española y Literatura**  
**CC. 092736281-4**  
**Registro SENESCYT: 7241168019**  
**Teléfono: 0958717798**

## DECLARATORIA DE AUTORÍA

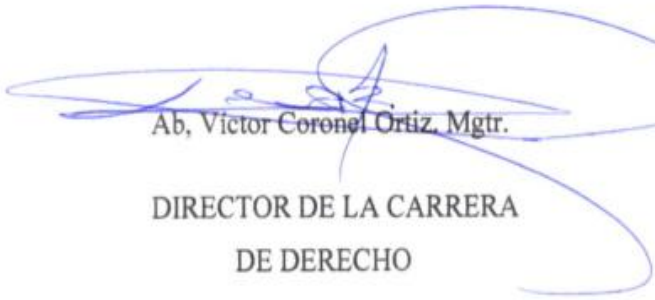
Yo, KATHERINE ESTEFANIA CORNEJO PONCE estudiante de la Carrera de Derecho de Universidad Estatal Península de Santa Elena, habiendo cursado la asignatura de Integración Curricular II, declaro la autoría del presente trabajo de investigación con el título **“ESTUDIO COMPARADO A LAS REGLAS DEL HABEAS DATA DE LAS LEGISLACIONES ECUADOR, ARGENTINA Y PERÙ 2024 ”**, desarrollado en todas sus partes por la suscrita estudiante 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.



KATHERINE ESTEFANIA CORNEJO PONCE

CC .240018724-7

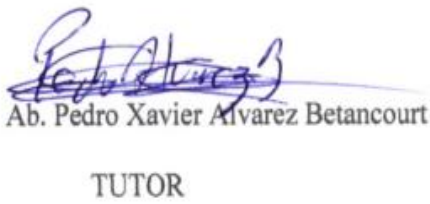
**TRIBUNAL DE GRADO**



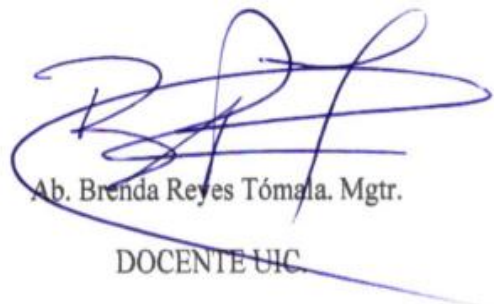
Ab, Victor Coronel Ortiz, Mgtr.  
DIRECTOR DE LA CARRERA  
DE DERECHO



Ab. Karen Díaz Panchana, Mgtr.  
DOCENTE ESPECIALISTA



Ab. Pedro Xavier Alvarez Betancourt  
TUTOR



Ab. Brenda Reyes Tómalá, Mgtr.  
DOCENTE UIC

## **DEDICATORIA**

*En primer lugar, a Dios, que me ha brindado una vida llena de alegrías y aprendizaje, permitiéndome vivir una muy grata experiencia en mi etapa universitaria.*

*A mi madre, esposo e hijos, por no soltar mi mano en todo este camino y quienes me motivaron para ser mejor cada día.*

***Katherine Cornejo***



## **AGRADECIMIENTO**

Agradezco infinitamente a la “Universidad Estatal Península de Santa Elena “en especial a la carrera derecho por su excelencia académica, que conjunto con sus prestigiosos docentes me formaron en esta etapa de estudiante, impartíendome sus conocimientos y experiencias que han sido cruciales para la consolidación de este trabajo.

A mi distinguido director Ab. Víctor Coronel Ortiz, Mgt, porque con sus gestiones logro que dentro de la carrera de derecho se nos imparta la materia de emprendimiento e innovación, conocimientos que es de gran relevancia para nuestro desarrollo como abogados en el campo laboral.

Y finalmente, a mi docente de UIC (unidad de integración curricular) Ab. Brenda Reyes Tomalá, Mgt, extendo mi más sincera gratitud, porque con su paciencia, dedicación y su inestimable guía, han sido pilares fundamentales en la dirección y enriquecimiento de esta investigación.

**Katherine Cornejo**

## ÍNDICE GENERAL

<i>PORTADA</i>	<i>I</i>
<i>CONTRAPORTADA</i>	<i>II</i>
<i>APROBACIÓN DEL TUTOR</i>	<i>III</i>
<i>CERTIFICACIÓN ANTIPLAGIO</i>	<i>IV</i>
<i>VALIDACIÓN GRAMATICAL Y ORTOGRÁFICA</i>	<i>V</i>
<i>DECLARATORIA DE AUTORÍA</i>	<i>VI</i>
<i>TRIBUNAL DE GRADO</i>	<i>VII</i>
<i>DEDICATORIA</i>	<i>VIII</i>
<i>AGRADECIMIENTO</i>	<i>IX</i>
<i>ÍNDICE GENERAL</i>	<i>X</i>
<i>ÍNDICE DE TABLAS</i>	<i>XIII</i>
<i>RESUMEN</i>	<i>XIV</i>
<i>ABSTRACT</i>	<i>1</i>
<i>INTRODUCCIÓN</i>	<i>2</i>
<i>CAPÍTULO I</i>	<i>4</i>
<i>PROBLEMA DE INVESTIGACIÓN</i>	<i>4</i>
1.1. Planteamiento del problema	<i>4</i>
1. 2. Formulación del problema	<i>6</i>
1. 3. Objetivo general y específicos	<i>6</i>
1.4. Justificación de la Investigación	<i>7</i>
1.5. Variables de investigación	<i>8</i>
1.6. Idea a defender	<i>8</i>
<i>CAPÍTULO II</i>	<i>9</i>
	<i>X</i>

<b>MARCO REFERENCIAL</b>	<b>9</b>
<b>2.1 Marco Teórico</b>	<b>9</b>
2.1.1 Origen y evolución del habeas data	9
2.1.2.-Naturaleza jurídica	12
2.1.3 Enfoques doctrinarios	15
2.1.4 Objeto y característica del habeas data	15
2.1.5. Tipos de habeas data	17
2.1.6 Las pretensiones del habeas data	18
2.1.7 Competencia y procedimientos del habeas data	19
2.1.8 Derecho a la libertad de acceder a los datos personales	20
2.2.9 Garantía procesal del habeas data	23
2.2.10 Inobservancia y su impacto en la justicia de datos	26
2.2.11 Pertinencia y procedibilidad de la garantía jurisdiccional del hábeas data	28
2.2.12 Clasificación de los datos y su pertinencia de modificación, aclaración o revelación según la Corte Constitucional ecuatoriana.	29
2.2.13 Habeas data en Ecuador Online	32
2.2.14 Dataservice	34
2.2.15 Tecnología de la información y comunicación (TIC)	36
2.2.16 Deficiencia de aplicación uniforme de principios de protección de datos.	37
<b>2.2 Marco Legal</b>	<b>38</b>
2.2.1 Constitución de la República del Ecuador	38
2.2.2 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional	42
2.2.3 Ley orgánica de protección de datos personales	46
2.2.4 Ley de comercio electrónico, firmas y mensajes de datos	48
2.2.5 Constitución de la República de Argentina	50
2.2.6 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional de Argentina	52
2.2.7 Ley de Acceso a la Información - Ley 27.275	53
2.2.8 Ley orgánica de protección de datos- Ley 25.326	58
2.2.9 Ley de comercio electrónico, firma y mensajes de datos	61
2.2.10 Constitución Política de Perú	61
2.2.11 Código Procesal civil de Perú	64
2.2.12 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional de Perú	67
2.2.13 Ley orgánica de protección de datos	67
2.2.14 Ley de comercio electrónico, firma y mensajes de datos	68
<b>2.3 Marco Conceptual</b>	<b>68</b>
<b>CAPÍTULO III</b>	<b>69</b>

<b><i>MARCO METODOLÓGICO</i></b>	<b><i>69</i></b>
<b>3.1. Diseño y tipo de investigación</b>	<b>69</b>
<b>3. 2 Recolección de la información</b>	<b>70</b>
<b>3. 3. Tratamiento de la información</b>	<b>72</b>
<b>3.4. Operacionalización de las variables</b>	<b>74</b>
<b><i>CAPÍTULO IV</i></b>	<b><i>75</i></b>
<b><i>RESULTADOS Y DISCUSIÓN</i></b>	<b><i>75</i></b>
<b>4.1 Análisis, interpretación y discusión de los resultados</b>	<b>75</b>
	<b>75</b>
<b>4.2 Verificación de la idea a defender</b>	<b>94</b>
<b><i>CONCLUSIONES</i></b>	<b><i>96</i></b>
<b><i>RECOMENDACIONES</i></b>	<b><i>97</i></b>
<b><i>BIBLIOGRAFÍA</i></b>	<b><i>98</i></b>

## ÍNDICE DE TABLAS

<b>Tabla #1</b> <b>Ámbito de aplicación material</b>	<b>12</b>
<b>Tabla #2</b> <b>Principios y alcance</b>	<b>13</b>
<b>Tabla #3</b> <b>Definiciones que se establece dentro de la sentencia</b>	<b>30</b>
<b>Tabla #4</b> <b>Población</b>	<b>70</b>
<b>Tabla #5</b> <b>Operacionalización de las variables</b>	<b>74</b>
<b>Tabla #6</b> <b>Matriz Comparativa</b>	<b>75</b>
<b>Tabla #7</b> <b>Matriz de Alcance y Protección del Habeas Data</b>	<b>76</b>
<b>Tabla # 8</b> <b>Matriz de Fundamentos Constitucionales y Legales</b>	<b>78</b>
<b>Tabla # 9</b> <b>Matriz de Aspectos Procesales</b>	<b>81</b>
<b>Tabla #10</b> <b>matriz normativa principal</b>	<b>85</b>
<b>Tabla # 11</b> <b>matriz definición de habeas data</b>	<b>86</b>
<b>Tabla # 11</b> <b>matriz de legitimación activa y pasiva</b>	<b>87</b>
<b>Tabla # 12</b> <b>matriz comparado de procedimiento del habeas data</b>	<b>88</b>
<b>Tabla # 13</b> <b>matriz ámbito de aplicación del habeas data</b>	<b>91</b>
<b>Tabla #14</b> <b>Matriz de Sujetos y Legitimación</b>	<b>93</b>

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

**ESTUDIO COMPARADO A LAS REGLAS DE HABEAS DATA  
DE LAS LEGISLACIONES DE ECUADOR,  
ARGENTINA Y PERÚ (2024)**

**Autora:** Katherine Cornejo

**Tutor:** Ab. Pedro Álvarez, Mgt.

**RESUMEN**

El enfoque ecuatoriano está fuertemente orientado hacia la protección de datos en el entorno digital, como respuesta a la creciente digitalización del Estado y del sector privado, las personas tienen el derecho de conocer, actualizar y rectificar la información recopilada por cualquier entidad, además, se establece un énfasis en la protección de datos sensibles, como los de salud o religión, y se ha creado una Autoridad de Protección de Datos que supervisa el cumplimiento de estas normas. En Argentina el mecanismo de Habeas Data permite a los ciudadanos exigir el acceso a sus datos, solicitar su rectificación o eliminación en caso de ser incorrectos o usados de manera ilegítima, la ley establece estrictos límites sobre la recolección de datos personales, destacando el principio de consentimiento informado. El país ha avanzado significativamente en la implementación de mecanismos para la protección de datos, con énfasis en el control y manejo por parte de entidades públicas y privadas, dentro de la ley peruana, al igual que en Ecuador y Argentina, otorga a los ciudadanos el derecho a acceder y modificar sus datos, además de imponer sanciones severas en caso de incumplimiento, asimismo, el Estado peruano ha establecido la Autoridad Nacional de Protección de Datos Personales, encargada de supervisar y garantizar el cumplimiento de la ley. En los tres países, el Habeas Data se concibe como un derecho fundamental vinculado con la protección de la privacidad y la autodeterminación informativa. Ecuador, Argentina y Perú han desarrollado marcos legales que otorgan a los ciudadanos la capacidad de controlar sus datos personales frente a la recolección y uso indiscriminado, los mecanismos para ejercer el Habeas Data son similares, permitiendo a los ciudadanos solicitar información, corregir datos erróneos o exigir la eliminación de datos innecesarios o perjudiciales.

**Palabras claves:** Habeas data, legislaciones, protección, datos, digital

## ABSTRACT

The Ecuadorian approach is strongly oriented towards data protection in the digital environment, as a response to the growing digitalization of the State and the private sector. People have the right to know, update and rectify the information collected by any entity. In addition, an emphasis is placed on the protection of sensitive data, such as health or religious data, and a Data Protection Authority has been created to oversee compliance with these standards. In Argentina, the Habeas Data mechanism allows citizens to demand access to their data, request its rectification or elimination if it is incorrect or used illegitimately. The law establishes strict limits on the collection of personal data, highlighting the principle of informed consent. The country has made significant progress in implementing mechanisms for data protection, with an emphasis on control and management by public and private entities. Peruvian law, as in Ecuador and Argentina, grants citizens the right to access and modify their data, in addition to imposing severe sanctions in case of non-compliance. Likewise, the Peruvian State has established the National Authority for the Protection of Personal Data, responsible for supervising and ensuring compliance with the law. In all three countries, Habeas Data is conceived as a fundamental right linked to the protection of privacy and informational self-determination. Ecuador, Argentina and Peru have developed legal frameworks that give citizens the ability to control their personal data against indiscriminate collection and use. The mechanisms for exercising Habeas Data are similar, allowing citizens to request information, correct erroneous data or demand the deletion of unnecessary or harmful data.

**Keywords:** Habeas data, legislation, protection, data, digital

## INTRODUCCIÓN

El Habeas Data es un mecanismo legal que permite a los individuos acceder, rectificar o eliminar información personal contenida en bases de datos, en Ecuador, Argentina y Perú, esta garantía está enfocado en proteger la privacidad y la integridad de los datos personales frente a su uso indebido por parte de instituciones públicas o privadas, aunque los tres países reconocen la importancia que este dentro de sus constituciones y normativas, cada uno ha desarrollado enfoques y regulaciones específicas que reflejan sus realidades jurídicas y contextos sociales.

Sin embargo, la ausencia de una legislación específica o suficientemente detallada puede generar incertidumbre tanto para los ciudadanos como para las empresas e instituciones que gestionan datos personales, los ciudadanos no saben con precisión qué derechos tienen o cómo ejercerlos de manera efectiva, mientras que las empresas no tienen claridad sobre cómo cumplir con las normativas, lo que puede llevar a violaciones de la privacidad o uso indebido de dato. Sin leyes específicas, es posible que no existan mecanismos adecuados para proteger los datos personales, esto puede resultar en una mayor vulnerabilidad frente a violaciones de la privacidad, como el uso indebido, el almacenamiento excesivo o la venta de datos sin consentimiento, la falta de regulación clara también dificulta la aplicación de sanciones efectivas contra las entidades que infringen los derechos de los ciudadanos.

El presente trabajo de investigación se propone abordar esta temática desde una perspectiva jurídica, enfocándose en el estudio comparado a las reglas de habeas data de las legislaciones de Ecuador, Argentina y Perú (2024) a través de un análisis exhaustivo del marco normativo vigente, la revisión de doctrina especializada y la matriz comparativa de cada país se busca evaluar las similitudes y diferencias en cada legislación.

Es determinante para el perfeccionamiento de la investigación el desarrollo de contenidos principales es así como en el Capítulo I, que se enfoca el planteamiento del problema, en donde resalta la defensa y protección de los datos personales, las similitudes y diferencias en las regulaciones del habeas data en las legislaciones de Ecuador, Argentina y Perú, en el Capítulo II, que lleva por nombre Marco Referencial, se indagara acerca del origen y



evolución del habeas data, naturaleza jurídica, enfoques doctrinales entre otros temas importantes.

Por otra parte, el Marco Metodológico se halla en el Capítulo III. en este constan las diversas vertientes que explican el fenómeno en el cual se centra el objeto de estudio, como el tipo de investigación, la metodología apropiada y los instrumentos a utilizar para el posterior tratamiento de la información, entre los tres países Ecuador, Argentina, y Perú para una mejor ilustración del tema.

Finalmente, el Capítulo IV incorpora el análisis, interpretación, y la matriz comparativa, en el que se consideran las similitudes y diferencias generadas a partir de las legislaciones entre los países mencionados.

## CAPÍTULO I

### PROBLEMA DE INVESTIGACIÓN

#### 1.1. Planteamiento del problema

La defensa y protección de los datos personales ha sido un desafío en la actualidad, por lo consiguiente el habeas data es una de las garantías constitucionales más considerada transcendentamente en la actualidad, nació como una maniobra de privacidad desde la década de los años 1970 y se ha extendido a las naciones latinoamericanas, entre ellas las que son objeto de estudio. Él jurista Pablo Contreras (2020) afirma que implementar una Constitución resulta un desafío en los sistemas jurídicos y que en el caso del derecho es fundamental a la autodeterminación informativa que partió del inicio de debates, en los que el derecho a la privacidad se consideraba insuficiente para proteger plenamente al individuo del cambio tecnológico. Dentro de la Constitución enfrenta dificultades al momento de crear leyes para la protección y acceso a los datos, y que la garantía a la autodeterminación informativa surgió como una respuesta a la insuficiencia y a la privacidad para proteger a las personas de los impactos del cambio tecnológico, en esta posición es importante, distinguir el carácter independiente del derecho a la protección de datos personales. Para entrar en entorno a la problemática se establece analizar el ámbito legal de cada país y como regula el habeas data en ellos, cabe destacar que actualmente la sociedad enfrenta unos de los desafíos que es, la difusa información sobre sus derechos al momento de acceder a sus datos, de acuerdo a la Ley de Garantías Jurisdiccionales y Control Constitucional y en la Constitución de la República del Ecuador, se hace mención que el habeas data garantiza la protección de documentos, fuentes de datos, bancos o archivos privados de información e informes sobre uno mismo o sus bienes. Estas normas no son exhaustivas, pero es posible que no aborden diversos aspectos de la garantía al acceso de datos personales y, por el contrario, son confusas o incluso ineficaces a la hora de proteger y a su vez garantizando el acceso de datos personales.

Una de las principales problemáticas jurídicas relacionadas con el habeas data en Ecuador, Argentina y Perú es la existencia de disparidades en la regulación y vacíos legislativos que afectan su aplicación efectiva. Aunque estos países reconocen el habeas data como una garantía constitucional, las leyes secundarias que lo desarrollan no son uniformes ni exhaustivas.

El Habeas Data enfrenta obstáculos en su aplicación práctica en los tres países. Muchos ciudadanos desconocen cómo ejercer su derecho o se enfrentan a procesos burocráticos y judiciales lentos, en algunos casos, como en Perú, se ha reportado que el acceso a la justicia para ejercer el habeas data es limitado debido a la saturación de los tribunales y la falta de recursos suficientes para hacer cumplir la ley de manera eficaz, esta situación impide que el garantía al habeas data sea verdaderamente accesible para todas las personas, especialmente aquellas en condiciones de vulnerabilidad. La supervisión y control de las normas de protección de datos en estos países presentan deficiencias importantes. Aunque existen organismos encargados de velar por el cumplimiento de las leyes, como la Autoridad Nacional de Protección de Datos en Perú y la Agencia de Acceso a la Información Pública en Argentina, la falta de recursos y capacidad técnica impide un monitoreo efectivo, en Ecuador, la creación de la Autoridad de Protección de Datos es reciente, y aún está en proceso de consolidación, lo que limita su capacidad de actuar con eficiencia y celeridad frente a las denuncias y violaciones de la normativa.

La creciente digitalización y el uso de tecnologías avanzadas, presentan una problemática jurídica que desafía las legislaciones del habeas data en los tres países, estas tecnologías permiten el procesamiento masivo de datos personales, muchas veces sin el consentimiento informado de los usuarios, lo que genera riesgos significativos para la privacidad, sin leyes específicas que regulen estos desarrollos tecnológicos, las personas están más expuestas a abusos, como la discriminación automatizada o la vigilancia masiva, esto resalta la necesidad de actualizar y expandir el marco legal del habeas data para abarcar estas nuevas realidades.

## **1. 2. Formulación del problema**

¿Cuáles son las similitudes y diferencias en las regulaciones del Habeas Data en las legislaciones de Ecuador, Argentina y Perú?

## **1. 3. Objetivo general y específicos**

### **Objetivo General**

Analizar las reglas del Habeas Data en las legislaciones de Ecuador, Argentina y Perú, comparando a través de las diferentes doctrinas similitudes, diferencias y su aplicación para determinar la protección de datos personales.

### **Objetivos Específicos**

- Identificar los aspectos clave que influyen en la protección de datos personales y el ejercicio de este derecho fundamental en cada país.
- Evaluar la efectividad de los mecanismos de protección establecidos en las leyes de Habeas Data de Ecuador, Argentina y Perú, con el fin de fortalecer la protección de la información personal de los ciudadanos.
- Analizar el impacto de las normativas del Habeas Data en la práctica, considerando cómo se aplican en la protección de datos personales, el acceso a la información y la toma de decisiones sobre el uso de los datos, con el objetivo de proponer recomendaciones para optimizar la protección de la privacidad en los tres países analizados.

#### **1.4. Justificación de la Investigación**

El tema “Estudio comparado a las reglas de habeas data de las legislaciones de Ecuador, Argentina y Perú” se basa en la protección de derechos fundamentales que permiten a los usuarios conocer, actualizar y rectificar datos personales que se encuentren en bases datos, sin embargo, existen diferencias en las reglas y disposiciones que regulan este derecho en cada país.

Este trabajo investigativo comprenderá que, aunque las legislaciones comparten principios generales, existen diferencias en cuanto a las leyes, el procedimiento, las sanciones, es decir, la problemática que existe al momento de querer un ciudadano acceder a sus datos personales, genéticos o bancarios que no permiten el acceso a la información siendo propietaria del mismo, por otra parte, existe una mala utilización arbitraria que hacen ciertas empresas públicas y privadas al distribuir datos personales sin autorización del usuario,

El estudio comparado de estas legislaciones muestra una evolución en cada país hacia una mayor protección de los datos personales y el fortalecimiento del habeas data como un mecanismo de salvaguardar la privacidad, a pesar de compartir un objetivo común dentro del Ecuador , existe un proceso del habeas data que se puede solicitar tanto en el ámbito judicial y administrativo ,esto permite que una de estas vías sea fácil para el procedimiento de los respectivos usuarios, por otro lado Argentina se enfrasca más en el ámbito judicial, esto implica tiempos más largos con la ventaja de garantizar un análisis más profundo por parte de los tribunales, y por último en Perú, se distingue al permitir el uso del habeas data para indagar la utilización de los datos , ampliando el derecho de conocer el propósito del tratamiento de la información .

## **1.5. Variables de investigación**

### **Univariable**

Estudio comparado a las reglas del Habeas Data.

## **1.6. Idea a defender**

El análisis comparado de las reglas de habeas data de las legislaciones de Ecuador, Argentina y Perú, enfrenta dificultades en la protección, acceso y la privacidad de los datos de los ciudadanos, esto implica estudiar el ámbito legal de cada país y como regula el habeas data en cada uno de ellos.

## **CAPÍTULO II**

### **MARCO REFERENCIAL**

#### **2.1 Marco Teórico**

##### **2.1.1 Origen y evolución del habeas data**

Después de la Segunda Guerra Mundial, en 1948, los estados debieron alcanzar un consenso sobre el respeto a los derechos humanos, desde entonces, han sido muy efectivos en la creación de leyes, tratados y acuerdos que aseguran la protección de estos derechos y han facilitado las relaciones entre naciones, dentro de la Declaración Universal de Derechos Humanos de 1948 ha incorporado el habeas data en las legislaciones de diversos países, promoviendo la implementación y el cumplimiento de los derechos humanos de los ciudadanos.

Los primeros inicios del Hábeas Data en América, se dieron en los Estados Unidos de Norteamérica, según la jurista García Rosalía propone que: con la llamada Privacy Act del 31 de diciembre de 1974, manifestaba que se encargaba de regular la protección de la privacidad de los ciudadanos estadounidenses, intentando dar al individuo mejor control en la recaudación, difusión y certeza de la información de él mismo. (Quíroz Papa de García, 2016)

En Ecuador, el habeas data apareció por primera vez en la Constitución Política de 1996, publicada en el Registro Oficial No. 969 el 18 de junio de ese mismo año, en la Sección II de las Garantías de los Derechos, párrafo III, se define en el artículo 30 como el derecho de toda persona a acceder a documentos, bases de datos e informes que contengan información sobre ella o sus bienes, ya sea en entidades públicas o privadas. También se garantiza el derecho a conocer el uso y propósito de dicha información. Asimismo, la persona puede solicitar a un funcionario o juez competente la actualización, corrección, eliminación o anulación de estos datos si son incorrectos o afectan sus derechos de manera ilegítima.

Se exceptúan los documentos reservados por razones de seguridad nacional. Gárate (2021) define este artículo como:

La redacción de una norma de contenido amplio, protectora en primer lugar de los derechos a ser informado sobre sí mismo y sobre sus bienes y a conocer el uso que se den a estos datos y su finalidad, los cuales pueden ser ejercidos no solo frente a las entidades públicas, sino también frente a las privadas.

Se destaca la importancia de una redacción clara y precisa al redactar un artículo legal, para definir adecuadamente las normas y derechos que se deben proteger, esto es esencial para evitar vacíos o conflictos legales cuando se plantea una acción por la vulneración de derechos en casos de habeas data, además, se establece un límite para el usuario al acceder a sus datos, asegurando que se le informe sobre el uso que se está dando a esa información, ya sea en el ámbito público o privado.

El habeas data en Ecuador tiene sus raíces en el desarrollo global de los derechos humanos y el reconocimiento de la privacidad como una garantía importante, este recurso jurídico surge como una respuesta al creciente uso de tecnologías de información y bases de datos que comenzaron a recopilar y almacenar información personal de los ciudadanos, su origen se vincula con la necesidad de proteger a las personas del uso indebido de sus datos por parte de entidades públicas y privadas, especialmente ante la preocupación por posibles abusos en la recopilación y manejo de la información.

En Ecuador, el primer acercamiento formal al habeas data se dio con la Constitución de 1998, que incluyó este recurso como una garantía constitucional para proteger los datos personales y la privacidad de los ciudadanos, este reconocimiento fue influenciado por las experiencias de otros países latinoamericanos, como Argentina y Brasil, que habían comenzado a adoptar mecanismos similares para la protección de datos personales. La inclusión del habeas data en esta Constitución fue un paso importante para establecer el derecho de los ciudadanos a conocer, actualizar y rectificar la información sobre ellos que se encontrara en bases de datos públicos o privados.

Con la Constitución de 2008, Ecuador fortaleció aún más esta garantía al establecer de manera explícita la acción de habeas data como una garantía fundamental en el artículo 92,



esta norma permite a cualquier persona acceder a datos e información que le concierne y que se encuentre en entidades públicos o privados, con el fin de conocer, actualizar, rectificar o eliminar información incorrecta o perjudicial, esta Constitución también se destacó por su enfoque en los derechos humanos, reconociendo explícitamente la protección de los datos personales como parte del derecho a la privacidad.

Actualmente, el habeas data está regulado en la Constitución de la República del Ecuador de 2008, publicada en el Registro Oficial No. 449, en la Sección Quinta, Acción de Habeas Data, en el artículo 92, a diferencia de la primera versión, esta actualización incluye cambios importantes, como la especificación de los derechos del titular para conocer la existencia de sus datos y el tratamiento electrónico de los mismos, también se establecen plazos de vigencia de los archivos y se adoptan medidas de seguridad acordes con los avances tecnológicos y de manera responsable.

Asimismo, se han desarrollado leyes como la Ley de Garantías Jurisdiccionales y Control Constitucional (LGJCC), cuyo Capítulo VI trata sobre la acción de habeas data con el objetivo de regular la jurisdicción constitucional. el artículo 42 de esta ley garantiza a toda persona el acceso a sus datos personales y establece el concepto de reparación integral, tanto material como inmaterial, según lo determine un juez, además, se asegura que estas disposiciones sean concordantes con la Constitución ecuatoriana. En consecuencia la Asamblea Nacional del Ecuador presentó el proyecto de la Ley Orgánica de Protección de Datos Personales (LODPP), que incluye 83 artículos, su principal objetivo es proteger los datos personales y garantizar el acceso de los usuarios, proporcionando principios, derechos, obligaciones y mecanismos de protección para su cumplimiento.

Tabla #1 *Ámbito de aplicación material*

<b>Personas naturales</b>	Que empleen esta información al llevar a cabo tareas del hogar o actividades familiares.
<b>Personas fallecidas</b>	Sin afectar lo dispuesto en el artículo 28 de esta Ley.
<b>Datos anonimizados</b>	Mientras no se pueda identificar al titular de los datos, en cuanto los datos dejen de estar separados o de ser anónimos, su manejo deberá cumplir con las obligaciones establecidas por esta Ley.
<b>Actividades periodísticas</b>	otros contenidos editoriales
<b>Datos personales</b>	Cuyo manejo esté regulado por normas especializadas de igual o superior jerarquía en temas de gestión de riesgos por desastres naturales, así como en seguridad y defensa del Estado.
<b>Datos o bases de datos establecidos para la prevención</b>	La prevención, investigación, detección o procesamiento de delitos, o la ejecución de sanciones penales, realizada por las autoridades estatales competentes en el ejercicio de sus funciones legales.
<b>Datos que identifican o hacen identificable a personas jurídicas</b>	Los datos personales relacionados con el contacto de profesionales, así como los de comerciantes, representantes, socios y accionistas de personas jurídicas, y funcionarios públicos, son accesibles al público y pueden ser tratados

Elaborado por: Katherine Cornejo

### 2.1.2.-Naturaleza jurídica

El habeas data de acuerdo con su naturaleza jurídica y doctrina constitucional, en Ecuador se aplica como una garantía dentro de la constitucionalidad, para proteger los derechos de la divulgación y accesibilidad de datos personales y cuya acción se determina mediante una resolución determinada por una apelación ante un superior.

Esta garantía protege derechos tales como los que se especifica en la tabla a continuación.

Tabla #2 Principios y alcance

<b>Principios</b>	<b>Alcance</b>
<p><b>HONRA</b></p> <p>Estima y respeto de la dignidad propia.</p> <p>Buena opinión y fama que se ha adquirido por la virtud y el mérito.</p>	<p>Salvaguarda a las personas de la divulgación de información que pueda perjudicar la buena reputación que han logrado.</p>
<p><b>INTIMIDAD</b></p> <p>Carácter del ámbito interno, personal, familiar de la persona.</p>	<p>Resguarda a las personas de cualquier interferencia en los asuntos de su vida familiar y personal, por cualquier medio o forma.</p>
<p><b>HONOR</b></p> <p>Virtud, probidad, gloria y buena reputación</p>	<p>Defiende a las personas de la divulgación de información que pudiera perjudicar su integridad, honestidad y buena reputación.</p>
<p><b>PRIVACIDAD</b></p> <p>Es el derecho del individuo para decidir por sí mismo en qué medida comparece con los demás sus pensamientos, sus sentimientos y los hechos de su vida personal</p>	<p>Defiende a las personas de la difusión o propagación de sus ideas o convicciones, y prohíbe la divulgación sin el consentimiento del titular de sus creencias, ideología, salud u orientación sexual. Esto se refiere a datos anteriores que pueden impactar su vida actual, resultando en un trato discriminatorio.</p>
<p><b>IDENTIDAD</b></p> <p>Conjunto de circunstancias que identifican quien y que es una persona</p>	<p>Defiende a las personas de la divulgación inexacta y incorrecta de su nombre, características étnicas, nacionalidad, procedencia, familia y expresiones culturales y sociales.</p>

**Elaborado por: Katherine Cornejo**

En términos generales, es un mecanismo o herramienta que protege los derechos constitucionales relacionados con la libertad de información, de manera más específica, se enfoca en la protección del derecho a la autodeterminación informativa, lo que implica la capacidad de cada persona para decidir sobre sus propios datos personales, garantizando su veracidad, registro y uso legal. Su naturaleza jurídica se considera un derecho genérico, ya que se compone de un conjunto de derechos específicos, de los cuales obtiene su contenido y fundamento.

Por su parte Alda García (2006), se refiere al habeas data como “Una petición que cualquier persona puede hacer, para protegerse de posibles perjuicios que conllevaría la mala utilización de datos que sobre sí misma se encontraren registrados por cualquier motivo”.

Este instituto establece su carácter de orden público al señalar que cualquier persona puede hacer una petición de habeas data, lo que implica que no hay discriminación por motivos de edad, etnia, religión o situación socioeconómica, su objetivo es proteger a las personas de posibles daños por la exposición pública de su información, el propósito de esta garantía es salvaguardar los derechos frente a un uso inadecuado de la información por parte de entidades públicas o privadas, aunque algunos podrían pensar que la protección del hábeas data se limita en ciertos casos, esto no es del todo cierto ya que existen reglas específicas, para activar la garantía del habeas data y dar cumplimiento en beneficio del perjudicado.

En la Constitución de 1998 ya se contemplaba la garantía constitucional del hábeas data, aunque el proceso debía realizarse ante el desaparecido Tribunal Constitucional, no existía una Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional y no era necesario que el afectado solicitara previamente la corrección a la entidad que poseía los datos antes de interponer la acción, ya que esta se presentaba de forma directa.

Al analizar con profundidad la naturaleza jurídica de la garantía del hábeas data, se comprende que está orientada a proteger los derechos subjetivos, como es el derecho a la libertad informativa, junto con los derechos inherentes a este, tales como: la intimidad, la privacidad y la identidad, si se vulnera el derecho a la libertad informativa, también se estarían afectando estos otros derechos, en especial el de la autodeterminación informativa, por lo que es importante distinguir entre libertad y autodeterminación informativas, la libertad informativa es lo genérico, mientras que la autodeterminación informativa es lo específico, ya que se refiere a la capacidad del individuo de decidir sobre la información que le pertenece dentro del marco de la libertad informativa.

Esto es la esencia de la protección, ya que lo que realmente se busca salvaguardar es el derecho subjetivo de la autodeterminación informativa, junto con el acceso a la información y su veracidad, si el juez comprende correctamente esta naturaleza, no debería haber problemas en el proceso, sin embargo, si no la entiende bien o no tiene claro su alcance, podrían surgir dificultades que podrían hacer que la garantía pierda su esencia o incluso su efectividad jurídica.

### **2.1.3 Enfoques doctrinarios**

La doctrina del habeas data protege la moralidad de las personas, según Enrique Falcón (2021), Actúa como una herramienta esencial para que la sociedad adquiera los conocimientos necesarios sobre la información que le concierne, permitiéndole acceder a sus registros en instituciones públicas o privadas, esto les permite ejercer su derecho a solicitar la corrección o actualización de datos.

Por esta razón es necesario destacar los tres derechos fundamentales para evitar el uso indebido de la información, protegiendo así el honor, la buena fe y la privacidad, que pueden verse afectados por el mal uso o la divulgación de datos incorrectos, inexactos o incompletos, derechos que están reflejados en la Constitución de la República del Ecuador, La Ley de Garantías y Control Constitucional y en la normativa de otros países para su comparación, dado que la característica más relevante de todo proceso de control constitucional es la anticipación de medidas, en todo caso sin que esta anule la bilateralidad ni el derecho a la contradicción, respetando el debido proceso y asegurando la validez, aunque se puedan adelantar plazos o reducir diligencias, manteniendo la efectividad y objetividad de esta garantía constitucional, sí se vulnerara con respecto al garantía del habeas data que es considerada un amparo constitucional, en este caso procedería establecer mediante el juez un control preventivo, ante un peligro o a su vez un control represivo confirmando la realización del acto, en estos casos la autoridad competente podrá rectificarlo o cesarlo.

### **2.1.4 Objeto y característica del habeas data**

El objetivo del habeas data es proteger a la sociedad de posibles abusos por parte de entidades que recopilan o distribuyen información personal, también ofrece una defensa legal frente a la discriminación u otras formas de violación de los derechos fundamentales, derivadas de la divulgación de información privada o íntima, especialmente debido al avance tecnológico, de este modo, se busca proteger los derechos fundamentales de tercera generación, como el derecho a la intimidad y a la privacidad, esta garantía es una herramienta adecuada y eficaz para garantizar que se respete este derecho, permitiendo que las personas puedan rectificar, actualizar, eliminar o anular sus datos personales almacenados en cualquier base de datos.

El habeas data es una garantía, que protege la información personal de los individuos, además de que mediante la normativa también permite el acceso a datos personales, en este sentido sus características principales son:

- Protección de datos personales: permite a los individuos acceder a sus datos personales almacenados en base de datos, así como quien posee y con qué propósitos se utilizan.
- Ratificación y actualización: proporciona el derecho a solicitar la corrección, actualización o eliminación de datos incorrectos, desactualizados o inexactos.
- Transparencia: garantiza que las entidades que recopilan y procesan datos personales lo hagan de manera transparente.
- Consentimiento: requiere que el procesamiento de datos personales se realice con el titular de los datos.
- Control y acceso: otorga a las personas el control sobre su información personal, permitiéndoles acceder a sus datos y conocer su uso y destino.
- Acción judicial: permite a los individuos presentar acciones judiciales para proteger sus derechos relacionados con sus datos personales, incluyendo la posibilidad de recurrir a tribunales si sus derechos son vulnerados.

Estas características garantizan que las personas mantengan un control efectivo sobre su información personal y que se respete su privacidad por lo que es importante destacar que la acción del hábeas data es una garantía que se ejerce mediante el derecho de petición reconocido en la Constitución, con un enfoque en la eficacia de las garantías jurisdiccionales. Es relevante señalar que esta garantía no se protege de manera aislada; su restauración se lleva a cabo a través de un juez competente, quien es responsable de hacer cumplir las resoluciones correspondientes, con un carácter autónomo, se centra en la Constitución Política y en la Ley de Control Constitucional, contando con estrategias específicas para su implementación.

### 2.1.5. Tipos de habeas data

Existen ciertas modalidades del derecho fundamental del habeas data, que se detallan a continuación:

- Habeas Data informativo: se refiere al acceso a la información personal, como los nombres de las personas.
- Habeas Data adictivo: incluye reformas que organizan o archivan información y datos.
- Corrección o Rectificación de Habeas Data: implica la corrección de información falsa, inexacta o inapropiada.
- Habeas Data Reservador: tiene como objetivo comprobar si la información está disponible.
- Habeas Data Especial o Suspensivo: permite eliminar datos almacenados en bases de datos o sistemas de información.

El habeas data individual se refiere a casos específicos, donde se conoce quiénes están tratando los datos y con qué propósito, esta modalidad es la más amplia y solo puede ser utilizada por los titulares de los datos en sus transacciones personales, por otro lado, el habeas data colectivo se aplica para proteger los datos personales de un grupo determinado o indeterminado de personas y puede tener efectos generales. Además existen otros tipos de habeas data que cabe mencionarlos para profundizar el tema:

- Habeas Data Impropio: se refiere a la obtención de información pública que normalmente se le niega al usuario o se difunde a través de medios tradicionales, como ocurre en Perú y Argentina, y que puede estar regulada bajo la protección de la Ley de Datos Personales.
- Habeas Data de Acceso a la Información: permite el libre acceso a datos públicos, aunque en algunos casos se restringe por motivos de seguridad del Estado, en Perú,

por ejemplo, se establecen acciones constitucionales para obtener información, manteniendo la esencia protectora del habeas data.

Estos diferentes tipos de habeas data reflejan la variedad de derechos de las personas en relación con la protección y accesibilidad a sus datos personales, cada modalidad busca garantizar que los individuos puedan ejercer un control efectivo y recibir un trato justo y seguro por parte de las entidades responsables.

### **2.1.6 Las pretensiones del habeas data**

La solicitud de acceso a la información es una garantía, el cual debe ser cumplido dentro de los plazos establecidos, este derecho permite al solicitante conocer o acceder a sus datos personales, y su ejercicio no debe ser restringido, solo regulado para mantener las formalidades legales correspondientes, un ejemplo claro de este derecho es la capacidad de solicitar información sin necesidad de justificar el motivo o causa, ya que la información personal es propia, confidencial y protegida por la normativa vigente.

La normativa jurídica que respalda esta garantía se encuentra en la Constitución, en los instrumentos Internacionales de los Derechos Humanos y en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (LOGJCC), estas normativas establecen el procedimiento a seguir para ejercer el derecho, siendo supletorios el Código Orgánico de la Función Judicial y el Código Civil, es fundamental entender qué derechos protege esta garantía para saber cuándo es conveniente ejercerla y tener la confianza de que se logrará proteger adecuadamente.

En cuanto a la Constitución y la LOGJCC, es importante recordar que estas normas tienen una jerarquía superior, siendo la Constitución la norma suprema del Estado y la LOGJCC una Ley Orgánica. Ambas buscan proteger los derechos fundamentales, y en el caso del habeas data, garantizar los derechos a la autodeterminación informativa y otros derechos relacionados, como señala el catedrático Jorge Zavala Egas (2010) “Las garantías jurisdiccionales y el papel de la Corte Constitucional son clave para garantizar la supremacía de la Constitución y asegurar que sus normas sean efectivas y vinculantes para todas las personas, autoridades e instituciones del país”.



Este autor también aborda el concepto de control difuso de constitucionalidad, el cual implica que todos los jueces deben estar atentos al cumplimiento y respeto de la Constitución, especialmente en lo relacionado con los derechos y su protección a través de las garantías jurisdiccionales, este deber es asumido implícitamente por los jueces, ya que, mientras duren los procedimientos, se consideran jueces constitucionales, es clave entender que los derechos protegidos por el habeas data, y en general por las garantías constitucionales, contienen aspectos subjetivos que, aunque no estén expresamente escritos en la norma constitucional, deben ser interpretados como parte de ella.

### **2.1.7 Competencia y procedimientos del habeas data**

El inciso tercero del Artículo 276 de la Constitución otorga al Tribunal Constitucional la facultad de intervenir en casos de denegación del habeas data, siendo este el punto central en cuestión. Esta competencia se ve reforzada por el Artículo 12, inciso tercero, de la Ley de Control Constitucional. Para que el Tribunal Constitucional pueda resolver sobre la negativa de conceder el habeas data, primero se debe presentar la acción ante un juez o tribunal de primera instancia en el lugar de residencia del responsable de la información o datos solicitados, tras la presentación, el juez o tribunal convocará una audiencia para el día siguiente, la cual deberá llevarse a cabo dentro de un plazo de ocho días, y emitir una resolución dos días después, en caso de que la resolución niegue el habeas data, este tiene su competencia restringida a las resoluciones que deniegan el habeas data, lo cual significa que los casos que llegan a su conocimiento son relativamente limitados, se observa que ni las partes involucradas en los procesos de habeas data ni el propio Tribunal Constitucional sustentan sus argumentos en el propósito esencial de esta garantía, que es, prevenir que el uso indebido de la información afecte la intimidad y otros derechos de la persona debido a la divulgación de datos incorrectos, incompletos o inexactos relacionados con ella o sus bienes.

Además, se señaló que fue aprobada una ley de derechos por el presidente y la ministra de Comunicaciones y Medios, Vianna Maino, el director también subrayó que 507 dependencias gubernamentales emplean los servicios de la Dinarp, tales como el Archivo de Información Ciudadana (FIC) y otros sistemas de interacción, esta herramienta contribuye a

mejorar y simplificar los procesos al permitir visualizar información sobre cédulas de ciudadanía y documentos electorales, optimizando así el funcionamiento. Su objetivo es garantizar un intercambio de información entre autoridades de manera controlada, segura, oportuna, transparente y en línea con las capacidades de cada una. Esto ayuda a mejorar los servicios corporativos a través de consultoría en línea, es fundamental enfocarse en los derechos de los interesados, mejorar la comunicación tanto dentro de la organización como con otras redes y organismos internacionales, además fortalecer la capacidad de liderazgo.

La Dirección de Protección de Datos Personales y la Dirección de Supervisión y Regulación, que colaboran en la aplicación de la Ley de Protección de Datos Personales y sus regulaciones asociadas, la Dirección de Protección de Datos Personales se enfoca en la aplicación de sanciones, gestionando un proceso trilateral y supervisando los informes que se presentan a la autoridad central encargada de la transparencia, el acceso a la información pública y la protección de la información privada.

Por otro lado, la Dirección de Fiscalización e Instrucción es la entidad responsable de monitorear el cumplimiento de las obligaciones y restricciones estipuladas en la Ley de Protección de Datos Personales y su reglamento. Esta dirección inicia procedimientos para imponer sanciones en casos de incumplimiento y dicta órdenes para la aplicación de dichas sanciones, asegurando la transparencia en el manejo de datos personales.

### **2.1.8 Derecho a la libertad de acceder a los datos personales**

Se garantiza a las personas el control y acceso a la información que las identifica o las hace identificables, este derecho permite a los individuos conocer qué datos personales están siendo recolectados, almacenados y procesados por entidades públicas o privadas, en la era digital actual, donde la información es un recurso de gran valor, proteger este acceso es esencial para salvaguardar la privacidad y evitar abusos, como la recolección indebida de datos o su uso para fines no autorizados.

En este sentido, las normativas internacionales, han establecido mecanismos para garantizar este derecho que exigen que las organizaciones proporcionen a los individuos acceso a sus datos personales cuando estos lo soliciten, esto incluye no solo la información misma, sino

también detalles sobre el propósito de su uso, la fuente de los datos y los terceros con quienes se han compartido. Este acceso no puede ser restringido sin una justificación legal clara, ya que forma parte del ejercicio como la privacidad y el control sobre la propia información.

El acceso a los datos personales también permite a los individuos corregir o eliminar información incorrecta o desactualizada, la posibilidad de solicitar la rectificación, actualización o eliminación de datos inexactos es un aspecto crucial de este derecho, pues garantiza la veracidad y la relevancia de la información que circula sobre las personas, este componente del derecho se conoce comúnmente como derecho de rectificación, y es esencial para evitar que datos falsos o erróneos causen perjuicios a los individuos, como en casos de discriminación laboral o social.

Además, el derecho de acceso a los datos personales juega un papel fundamental en la transparencia y la rendición de cuentas de las instituciones que gestionan dicha información, al garantizar que los individuos puedan acceder a sus datos, se promueve un entorno en el que las organizaciones deben ser claras sobre sus políticas de manejo de datos y responsables ante los usuarios contribuye a crear confianza en los servicios digitales, ya que las personas sienten mayor seguridad al saber que tienen la posibilidad de verificar cómo se está utilizando su información.

El derecho a la libertad de acceder a los datos personales es un componente esencial de los derechos de privacidad en la sociedad digital actual, su ejercicio permite a los individuos tener control sobre su información, facilita la corrección de datos inexactos, y promueve la transparencia en el manejo de datos personales, este derecho no solo protege a los individuos de potenciales abusos, sino que también fomenta prácticas responsables en el tratamiento de la información por parte de las organizaciones, garantizando así un equilibrio entre el uso de los datos y la protección de los derechos fundamentales de las personas.

De acuerdo con el Artículo 276, inciso tercero de la Constitución, y el cuarto inciso del Artículo 41 de la Ley de Control Constitucional, el Tribunal tiene una competencia limitada a las resoluciones que rechazan el habeas data, lo cual implica que los casos que llegan a su análisis son relativamente pocos, porque el habeas data se configura como un proceso

autónomo especializado y expedito en proteger la intimidad y otros derechos de la persona frente al uso indebido de información o la divulgación de datos incorrectos, incompletos o inexactos que le conciernan.

Asimismo, se informó sobre la aprobación de una ley de derechos por parte del presidente y la ministra de Comunicaciones y Medios, Vianna Maino, el director destacó que 507 dependencias gubernamentales utilizan los servicios de la Dinarp, como el Archivo de Información Ciudadana (FIC) y otros sistemas de interacción, esta herramienta facilita y mejora los procesos permitiendo la visualización de información sobre cédulas de ciudadanía y documentos electorales, optimizando el funcionamiento de las instituciones públicas, su objetivo es asegurar un intercambio de información entre autoridades de forma controlada, segura, oportuna y transparente, según las capacidades de cada institución esto contribuye a mejorar los servicios corporativos mediante consultoría en línea.

El 26 de mayo de 2021 se aprobó la primera Ley de Protección de Datos del Ecuador, determinando los lineamientos y principios que se deben implementar para garantizar la privacidad de los ciudadanos.

Por otro lado, regula el derecho de acceso y elección de los datos recopilados para permitirles hacer frente a los desafíos del mundo digital.

Sin embargo, esta ley entró en vigor el 26 de mayo de 2023, puesto que se dio el plazo otorgado a las empresas y organizaciones de procesamiento de datos para actualizar sus aplicaciones de acuerdo con la ley en cuestión.

El derecho a la libertad de acceder a los datos personales también está estrechamente vinculado con la protección de la dignidad humana, los datos personales reflejan aspectos de la identidad, comportamientos y preferencias de los individuos, permitiendo a las personas acceder a esta información no solo para asegurar la transparencia, sino que refuerza el respeto a la autonomía individual, la capacidad de conocer y controlar qué información sobre uno mismo es recolectada y cómo se utiliza, de esta manera el usuario tiene conocimiento sobre la manipulación o el uso indebido de sus datos, cumpliendo así el principio de confidencialidad y asimismo la seguridad de los datos personales.

Es importante mencionar otros aspectos clave que complementan el derecho al acceso libre de datos, garantizado por el habeas data, como es el acceso gratuito y no discriminatorio, la finalidad de uso de los datos y que medidas de seguridad son adoptadas para proteger la información. También se refuerzan los mecanismos de protección contra accesos no autorizados, filtraciones o mal uso de la información, sobre todo las leyes de protección de datos suelen establecer obligaciones específicas para las entidades que gestionan esta información, como notificar a los usuarios en caso de violaciones de seguridad a través de correos electrónicos o demás medios de comunicación. Esto asegura que el acceso no comprometa la integridad y privacidad de los datos, creando un entorno más seguro para la gestión de información personal.

En la práctica, el ejercicio del derecho de acceso a los datos personales presenta desafíos, especialmente con el crecimiento de las tecnologías digitales y el uso masivo de datos, muchas veces, las personas no son conscientes de cuánta información están proporcionando a través de sus interacciones en línea o de cómo las empresas recopilan y procesan esos datos. Además, el proceso para acceder a esta información puede ser complicado y burocrático, lo que limita su efectividad. Es esencial que las normativas de protección de datos establezcan procedimientos claros y accesibles para que los usuarios puedan ejercer este derecho de forma efectiva y sin obstáculos innecesarios, promoviendo políticas y directrices que buscan equilibrar el uso legítimo de los datos con la protección de los derechos fundamentales. En un mundo cada vez más globalizado e interconectado, garantizar el acceso a los datos personales es esencial para mantener un equilibrio entre el desarrollo tecnológico y la protección de los Derechos Humanos, permitiendo a los individuos ser dueños de su propia información y preservar su privacidad frente a posibles abusos.

### **2.2.9 Garantía procesal del habeas data**

El hábeas data es una garantía con un mecanismo procesal que permite a los ciudadano la defensa de la intimidad, la privacidad y demás derechos conexos, del mismo modo esta garantía procesal permite realizar un análisis comparativo de como se ha implementado el habeas data en diferentes países de América latina buscando asegurar el acceso a la

información y la protección de los datos personales, fundamentándose en la doctrina que establece el derecho de los ciudadanos a controlar, acceder y gestionar la información que les concierne, esta forma de intimidad no se ve como un valor intersubjetivo, sino como una autodeterminación del individuo en sus relaciones con otros ciudadanos y con el poder público. En este marco, el hábeas data cumple un papel clave en la protección de la información personal, ya que garantiza el derecho a la autodeterminación informativa o libertad informática, pues es un requisito para la protección de otras libertades. Puesto que evita que la información sobre las personas sea utilizada en su contra, vulnerando sus derechos y libertades.

De acuerdo con la Resolución No.19 La Corte Constitucional del Ecuador (CCE) respalda como la autodeterminación informativa, así como la privacidad e intimidad de los datos personales ,en este sentido, el habeas data se posesiona como una herramienta procesal frente a los desafíos que presentan las nuevas tecnologías, considerando que el avance de la inteligencia artificial cada vez afecta más la seguridad de la información y el tratamiento de los datos personales, debido a su circulación ilimitada y el acceso libre en una sociedad conectada, el estudio y aplicación del habeas data permite ejercer correctamente los derechos de acceso, rectificación, cancelación y oposición relacionados con la protección de la información personal.

Se destacan dos aspectos clave en el tratamiento de datos personales: el control sobre la información y el deber de respetar el derecho fundamental a la protección de datos en la sociedad es crucial que el manejo de los datos se adhiera a principios que protejan estos derechos fundamentales, además, dado que los datos personales son diversos, es esencial establecer límites y controles en el tratamiento de información sensible para garantizar su cumplimiento efectivo.

Son datos que pertenecen a la esfera personal o íntima de una persona –es una información que se reserva para uno mismo o para los más cercanos- y su conocimiento afecta gravemente a la intimidad personal y familiar y al libre desarrollo de la personalidad, teniendo un enorme potencial discriminador. (Troncoso, 2010)

Por tanto, también es importante centrar el debate en la preocupación sobre el desconocimiento del contenido de este derecho fundamental y las facultades que se atribuyen

a los titulares de la información personal frente al tratamiento ilícito que puede resultar en la sociedad de la información. En todo caso, si bien la protección de datos personales debe acompañarse atendiendo a la mayor o menor cercanía con otros derechos fundamentales, es esencialmente importante priorizar su sensibilización tanto en el ámbito público como privado. En este sentido, frente al tratamiento de la información personal, los responsables del tratamiento deben respetar una serie de principios y deberes que componen este derecho fundamental. En este plano, se destaca la confianza, la seguridad, incluida la intimidad, privacidad y confidencialidad, como elementos esenciales en el tratamiento de la información.

Por otra parte, no es relevante en este estudio realizar un diagnóstico de la cronología del origen del habeas data, pero sí es necesario conceptualizar las causas que promovieron el surgimiento de esta garantía constitucional frente a las nuevas tecnologías. Así, en primera instancia, la doctrina apunta que:

La inquietud sobre las agresiones a la intimidad que podían desprenderse por usos indebidos de las NT y las TIC (...) suscitó un progresivo debate entre los teóricos del derecho, que luego influyó en algunas decisiones jurisprudenciales y se tradujo también en previsiones constitucionales y legislativas sobre la materia. La temática relativa al “habeas data” (...) pretendía establecer una garantía procesal frente a la vulneración de la privacidad realizada a través de usos indebidos o abusivos de equipos informáticos (Perez, 2017).

Otros autores agregan que esta garantía comprende un proceso constitucional o un recurso protectorio del derecho de autodeterminación informativa o derecho a la protección de los datos personales frente a posibles excesos del poder de registración precisamente de la información de carácter personal. Así también, como se ha mencionado anteriormente, del habeas data se desprenden los derechos acceso, rectificación, cancelación y oposición (ARCO) que configuran un conjunto de facultades destinadas a tutelar el tratamiento de la información personal; y, en suma, garantizar el ejercicio, control y poder de disposición de los datos personales.

### **2.2.10 Inobservancia y su impacto en la justicia de datos**

La inobservancia en el manejo de datos personales ha generado precedentes significativos que afectan gravemente a la justicia de datos y a la protección, en varios casos, tanto a nivel nacional como internacional, los tribunales han señalado cómo el mal manejo de la información personal puede vulnerar el derecho a la privacidad y a la autodeterminación informativa, la jurisprudencia ha enfatizado que la inobservancia de los principios de protección de datos como la transparencia, la finalidad específica y el consentimiento informado puede derivar en situaciones de abuso, afectando la integridad de los individuos y la confianza en el sistema judicial.

Es por ello que la situación actual genera incertidumbre y falta de previsibilidad en la aplicación del habeas data, lo que dificulta el acceso efectivo de las personas a esta herramienta constitucional para la protección de sus datos personales, la Corte ha establecido que, en casos donde exista controversia sobre el inicio de la aplicación de esta garantía, los precedentes sobre la improcedencia del habeas data son vinculantes para los jueces constitucionales, en casos de emitir fallos en acciones de habeas data en estas circunstancias se corre el riesgo de vulnerar derechos fundamentales, lo que provoca inseguridad jurídica y debilita la justicia de datos en Ecuador, pese a ser una normativa de cumplimiento obligatorio.

Cabe considerar que uno de los precedentes más relevantes ha sido el caso de la recolección indiscriminada de datos personales por parte de entidades públicos o privados sin el consentimiento de los titulares, la Corte Constitucional de Ecuador, en varias resoluciones, ha advertido que esta práctica constituye una violación directa del derecho a la privacidad, en estos casos, la inobservancia de la normativa sobre datos personales ha permitido la creación de perfiles sin autorización, el uso de datos para finalidades distintas a las previstas y, en algunos casos, su venta a terceros, la falta de supervisión adecuada y la carencia de sanciones efectivas han debilitado la confianza de los ciudadanos en la protección de sus datos.



Otro precedente significativo en la jurisprudencia se refiere al acceso no autorizado a datos personales sensibles, especialmente en contextos de salud, identidad y antecedentes judiciales, la Corte Interamericana de Derechos Humanos ha establecido que la exposición indebida de estos datos puede generar graves daños a las personas, incluyendo discriminación, estigmatización y vulneraciones a los derechos, un ejemplo notable fue el uso indebido de datos de pacientes en instituciones de salud, donde la información fue divulgada sin el consentimiento del paciente, afectando su privacidad y generando consecuencias psicológicas y sociales negativas, estos casos destacan la importancia de implementar estrictas medidas de protección y supervisión.

En el ámbito de la justicia de datos, la falta de un adecuado proceso de rectificación y eliminación de datos erróneos también ha sido objeto de análisis judicial. Precedentes en la Corte Constitucional ecuatoriana han señalado que la negativa a corregir datos incorrectos o desactualizados puede llevar a decisiones judiciales injustas, afectando derechos como el acceso al empleo, la reputación y el crédito financiero, en una economía y sociedad cada vez más digitalizadas, esta inobservancia puede tener efectos devastadores en la vida de las personas, consolidando prejuicios y perpetuando errores sin justificación ha determinado que las autoridades responsables de los datos deben garantizar mecanismos eficaces para corregir y actualizar la información de forma oportuna.

Los precedentes de inobservancia en la justicia de datos también reflejan fallas en la implementación de marcos legales adecuados para la protección de datos personales. La ausencia de legislación específica o de instituciones encargadas de supervisar el cumplimiento de estas normas ha facilitado situaciones de abuso y vulneración de derechos, en Ecuador, la Ley de Protección de Datos Personales busca subsanar estas deficiencias, pero aún enfrenta desafíos en su aplicación efectiva, la jurisprudencia ha indicado que la falta de implementación robusta de estas normativas afecta gravemente la justicia de datos, perpetuando un escenario de inseguridad y desconfianza en el tratamiento de la información personal.

La falta de cumplimiento de los precedentes jurisprudenciales afecta gravemente la justicia en relación con los datos en Ecuador, la Corte Constitucional ha establecido en varias

sentencias que las autoridades judiciales tienen la obligación de seguir los precedentes sobre la aplicación del habeas data, especialmente en casos de negativas tácitas y en los distintos tipos de garantías, como las informativas, correctivas, de reserva y cancelación, cuando los jueces no siguen estos precedentes al resolver acciones de habeas data, se vulneran derechos como la seguridad jurídica y la debida motivación. Por ejemplo, si se niega un habeas data correctivo sin aplicar los criterios jurisprudenciales sobre los diferentes tipos de habeas data, esto genera incertidumbre y falta de predictibilidad en su aplicación.

### **2.2.11 Pertinencia y procedibilidad de la garantía jurisdiccional del hábeas data**

Frente a la procedibilidad del habeas data, es necesario definir ciertas conceptualizaciones referentes al componente del dato personal, dato sensible, e información sensible reservada al público. De lo antes aclarado, podremos obtener uno de los dos aspectos para realizar una comparativa a manera de espejo entre los requisitos para acceder a la garantía del habeas data, obtenido del diccionario de la Real Academia de la Lengua Española, conceptualizando a la garantía jurisdiccional de habeas data como la:

Acción constitucional que puede ejercer cualquier persona incluida en un registro de datos para acceder al mismo y recabar la información que le afecte, así como para solicitar su eliminación o corrección si tal información fuera falsa o estuviera desactualizada. (Pacheco, 2014)

Mientras que por otro lado la tipología de datos según su naturaleza, uso, alcance, fundamenta la garantía aplicable a cada tipo de dato, así como las obligaciones legales de quienes lo procesan a nivel de sensibilidad. Considerando de que estos requisitos formales, está condicionada a la negativa de acceso a la información perteneciente al solicitante contando también el silencio como una negativa tácita a la solicitud.

En Ecuador el cuerpo jurídico encargado de regular el acceso a las garantías jurisdiccionales, recae sobre la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, la misma que brinda lineamientos específicos sobre los cuales se puede proponer la acción de habeas data estableciendo los casos en los que se puede interponer la acción tal como lo tipifica en su Art. 23:

Cuando se niega el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o estén en poder de personas naturales o jurídicas privadas.

Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos.

Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente. (Asamblea Nacional, 2009)

De acuerdo con este artículo la importancia de la tipología en el habeas data consiste en tener presente tres puntos importantes como:

- Diferenciación de derechos: que mide el nivel de protección, variando según el tipo de dato; por ejemplo, los datos sensibles tienen mayores restricciones que los públicos.
- Consentimiento informado: guía las obligaciones de las entidades que tratan los datos en términos de obtener y documentar la autorización del titular.
- Acciones correctivas: facilita la identificación de que tipo de dato ha sido vulnerado para adoptar medidas adecuadas, como supresión y actualización.

#### **2.2.12 Clasificación de los datos y su pertinencia de modificación, aclaración o revelación según la Corte Constitucional ecuatoriana.**

La Corte Constitucional ecuatoriana ha desarrollado una clasificación de los datos personales y ha definido criterios específicos para su protección y la pertinencia de su modificación en el marco del derecho hacia la garantía del habeas data.

En este sentido se deduce que para poder accionar la garantía jurisdiccional del habeas data se debe tener claros, varios puntos, entre ellos están la definición, modificación, pertinencia, datos públicos y semiprivados, se resalta que únicamente protege aquellos datos que cumplan con una función informativa sobre el derecho de a quien se refiere. Cabe mencionar que se debe indicar también cuáles son los límites de la información si es susceptible a cambio, modificación o eliminación, y a criterios de la Corte Constitucional desarrollados en sentencia.

Dentro de las sentencias desarrolladas por el antes mencionado órgano jurisdiccional se encuentran terminologías que hacen referencia de los datos personales, datos sensibles e

información reservada, pero nace la interrogante si toda esta información es susceptible de aplicación de una garantía jurisdiccional de habeas data. Es entonces cuando nace la necesidad de acudir tanto a la doctrina como a la jurisprudencia, es aquí donde se encuentran las siguientes definiciones:

*Tabla #3 Definiciones que se establece dentro de la sentencia*

<b>DATOS PERSONALES</b>	Información que puede ser relacionada con una persona física, identificable por un nombre, edad cedula, dirección, cedula, identidad electrónica, etc., estos datos pueden dar con la identificación y la singularización de una persona en concreto, delimitando en ella únicamente la identificación personal.
<b>INFORMACIÓN TRATADA</b>	Tipo compuesto de información en la cual guarde dos aspectos, el primero sea la identificación de la persona, y la segunda sea cualquier aspecto que periferia a consideración del interesado o productor de dicha información mantener en carácter de oculto hasta el momento de la decisión del productor compartirla con una persona o grupo de personas en específico dejando salvo la integridad del derecho ajeno.
<b>INFORMACIÓN APARTADA</b>	Aquella que se encuentra temporal o indefinidamente fuera del alcance publico esto motivado por el daño que podría ocasionar la divulgación de esta a las personas, al interés público.

**Fuente:** sentencia 4 10-22-ep/23,2023

**Elaborado por:** Katherine cornejo

En Ecuador, ha desarrollado una importante doctrina sobre la clasificación de los datos personales y su relevancia en cuanto a su modificación, aclaración o revelación, el análisis de esta clasificación permite establecer diferentes niveles de protección y derechos aplicables según el tipo de dato, en general, los datos se dividen en tres categorías principales tales como datos personales básicos, datos personales sensibles y datos de acceso público, esta clasificación responde a la necesidad de garantizar la protección de la privacidad de las personas y de regular el acceso a su información, permitiendo el ejercicio de los derechos fundamentales de rectificación, actualización y eliminación.

Los datos personales básicos son aquellos que identifican o hacen identificable a una persona, como su nombre, dirección, número de teléfono o correo electrónico. Según la jurisprudencia de la Corte Constitucional, este tipo de datos puede ser objeto de modificación

o aclaración si la persona afectada considera que la información es incorrecta o está desactualizada. El derecho a la rectificación es crucial en este contexto, ya que permite mantener la veracidad de la información y evita perjuicios en casos donde datos erróneos puedan afectar a la persona en procesos legales, trámites administrativos o relaciones comerciales. La Corte establece que este derecho debe ser garantizado por todas las entidades, públicas o privadas, que gestionen datos personales.

En cuanto a los datos personales sensibles, ha sido enfática en su protección reforzada debido a su naturaleza íntima y la posibilidad de causar discriminación o daños a la dignidad de la persona, estos datos incluyen información sobre origen étnico, salud, orientación sexual, creencias religiosas y opiniones políticas, la revelación de estos datos está sujeta a restricciones más estrictas, y su modificación o eliminación debe estar siempre respaldada por el consentimiento expreso del titular de los datos esto también ha señalado que cualquier tratamiento indebido de esta información puede ser objeto de sanciones legales, dado el impacto potencial en los derechos fundamentales de los individuos.

Por otro lado, los datos de acceso público son aquellos que, por su naturaleza o por disposición legal, pueden ser consultados por cualquier persona sin necesidad de autorización previa, estos incluyen, por ejemplo, información contenida en registros públicos o boletines oficiales. Sin embargo, la Corte Constitucional ha subrayado que la existencia de este tipo de datos no implica una carta abierta para su uso indiscriminado, si bien su revelación no requiere el consentimiento del titular, el uso de esta información debe respetar los principios de proporcionalidad y finalidad, evitando que se utilice para fines que puedan afectar la privacidad o la dignidad de la persona. En caso de uso indebido, el titular de los datos tiene derecho a solicitar una aclaración o corrección.

La pertinencia de modificación, aclaración o revelación de los datos personales según la Corte Constitucional ecuatoriana depende de la categoría a la que pertenezcan dichos datos, esta clasificación es fundamental para establecer el nivel de protección y los mecanismos legales aplicables, la jurisprudencia de la Corte ha sido clara en la defensa de los derechos de los ciudadanos frente al tratamiento de sus datos personales, promoviendo un marco que busca equilibrar el derecho a la información con la protección de la privacidad y dignidad

de las personas, de esta manera, se garantiza un manejo adecuado de la información en línea con los principios constitucionales de Ecuador y los estándares Internacionales de los Derechos Humanos.

### **2.2.13 Habeas data en Ecuador Online**

En Ecuador, la recolección de datos en línea es un proceso común en el que las páginas web recopilan información de los usuarios para diversas finalidades, como mejorar la experiencia del usuario, personalizar contenidos, publicidad y realizar análisis de comportamiento, sin embargo, esta práctica puede resultar problemática si no se lleva a cabo de manera transparente y ética, consecuentemente la falta de información clara sobre qué datos se están recolectando y cómo se usarán, puede llevar a la vulneración de la protección de datos.

Además, muchas páginas web utilizan herramientas de seguimiento, análisis que registran información sobre las interacciones del usuario con el sitio, esto incluye detalles como las páginas visitadas, el tiempo de permanencia y los clics realizados, sin una política de privacidad bien definida, en esta circunstancia los usuarios pueden no estar al tanto de cómo está siendo utilizada sus datos en línea, lo que socava su derecho a la privacidad. Así mismo los usuarios deben ser capaces de entender, de manera sencilla, cómo sus datos podrían ser utilizados y por quién, la opacidad en este aspecto no solo es éticamente cuestionable, sino que también puede tener repercusiones legales.

Otro factor importante es el consentimiento, este un pilar fundamental en la protección de datos personales, dentro de la navegación online, las páginas deben obtener el consentimiento explícito de los usuarios antes de recolectar y procesar sus datos, esto significa que los usuarios deben ser informados de manera clara sobre lo que implica su consentimiento y qué datos específicos se están recopilando, si las páginas no hacen esto están vulnerando el derecho a la protección de datos personales.

Este paso debe ser otorgado de manera activa, lo que implica que los usuarios deben tomar una acción específica para indicar su acuerdo, como marcar una casilla o hacer clic en un botón, esto no debe considerarse válido un consentimiento obtenido mediante casillas

preseleccionadas o suposiciones, ya que esta práctica no solo es engañosa, sino que también va en contra de las normativas que protegen la privacidad de los usuarios.

Las consecuencias de no obtener el consentimiento adecuado pueden ser severas, las empresas pueden enfrentar sanciones legales, así como daños a su reputación y la pérdida de confianza del consumidor, los usuarios deben tener el poder de decidir qué datos están dispuestos a compartir y que empresas tienen la responsabilidad de respetar esa decisión.

Además, es importante resaltar que este sitio web proporciona que a los usuarios tengan la opción de retirar su consentimiento en cualquier momento, este derecho a la revocación debe ser fácil de ejercer y debe ser claramente explicado, sin esta opción, los usuarios se sienten atrapados en acuerdos de consentimiento que pueden no haber comprendido completamente, lo que representa una violación a la garantía constitucional del habeas data.

El derecho de acceso y rectificación es un componente esencial del habeas data que permite a los usuarios revisar la información que las empresas tienen sobre ellos, esto incluye el derecho a solicitar copias de sus datos personales y obtener detalles sobre cómo se están utilizando, sin embargo, muchas páginas web no proporcionan mecanismos claros y accesibles para que los usuarios puedan ejercer este derecho, lo que puede llevar a la frustración y a la desconfianza.

Las empresas deben establecer procedimientos simples y transparentes para que los usuarios puedan solicitar acceso a sus datos, esto implica no solo tener una política de privacidad comprensible, sino también proporcionar un canal de comunicación efectivo donde los usuarios puedan hacer estas solicitudes, por otra parte, la falta de este tipo de accesibilidad puede interpretarse como una evasión de la responsabilidad sobre los datos tratados.

Dentro del derecho de rectificación permite a los usuarios corregir cualquier información inexacta o desactualizada que las empresas o sitios web tengan sobre ello, esto es particularmente importante en un mundo donde los datos pueden cambiar con frecuencia, deben facilitar el proceso de rectificación, asegurando que los usuarios puedan actualizar su información sin complicaciones, por lo que es crucial que sean proactivas en la gestión de

los datos personales, esto se comprende en no solo responder a las solicitudes de acceso y rectificación, sino también revisar periódicamente sus propias prácticas de manejo de datos.

#### **2.2.14 Dataservice**

Uno de los mayores riesgos es el manejo de información personal sin obtener el consentimiento explícito de las personas, en Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) establece que cualquier tratamiento de datos personales debe realizarse con el consentimiento informado de los titulares, en ocasiones las empresas que manejan grandes volúmenes de datos no informan adecuadamente a las personas sobre cómo se recopilan, almacenan y utilizan sus datos, lo que representa una vulneración de su derecho a la privacidad.

En muchos casos, los sistemas de gestión de datos, como los de Dataservice, pueden ser vulnerables a accesos no autorizados por parte de empleados o hackers, esto puede ocurrir si las medidas de seguridad no son lo suficientemente robustas, lo que permite la filtración de datos sensibles como números de cédula, direcciones, y detalles bancarios, esta situación puede exponer a los ciudadanos a riesgos como el robo de identidad o fraudes.

A pesar de los avances en la legislación, algunas empresas en Ecuador aún no cumplen completamente con las normativas de almacenamiento y protección de datos personales, Asimismo si la información se guarda en sistemas no cifrados o en servidores vulnerables, puede ser fácilmente accesible para actores maliciosos, esto aumenta el riesgo de que la información personal sea divulgada sin el consentimiento del titular. El tratamiento de los datos personales debe estar claramente delimitado, indicando la finalidad para la cual se recogen, en ocasiones estas instituciones no informan de manera clara y transparente los fines específicos para los cuales se utilizarán los datos, lo que puede derivar en su uso inapropiado o comercialización sin el conocimiento de las personas afectadas.

Las bases de datos personales, especialmente aquellas con información detallada sobre preferencias y hábitos de consumo, son valiosas para el marketing. Sin embargo, el uso indebido de estos datos para fines publicitarios sin el consentimiento de los individuos puede ser una clara vulneración de la privacidad. Además, las estrategias de segmentación basadas



en información personal pueden llevar a que los consumidores reciban ofertas no deseadas o sean objeto de prácticas de marketing agresivas.

La recolección masiva de información personal puede ser problemática cuando no se lleva un control adecuado de los datos, si estos sitios recopilan grandes cantidades de datos sin restricciones claras sobre qué información es relevante y necesaria, se corre el riesgo de que se recojan datos sensibles sin una justificación válida, lo que puede comprometer la privacidad de los individuos.

Dataservice o servicios de datos en Ecuador son plataformas y empresas que se encargan de recopilar, almacenar y gestionar grandes cantidades de información de los ciudadanos, a menudo con fines comerciales o de seguridad, estas entidades, en su mayoría privadas, adquieren y procesan datos personales de diversas fuentes, incluidas redes sociales, registros públicos y otras bases de datos accesibles en línea, cuando la obtención o el tratamiento de estos datos se realiza sin el debido consentimiento o sin informar claramente a los titulares de los datos, observando claramente la vulneración del derecho a la privacidad y a la garantía jurisdiccional del habeas data, pues el ciudadano desconoce sobre la utilización de su información en esta plataforma de Dataservice.

Uno de los principales riesgos de Dataservice en Ecuador es que muchos de ellos operan sin una supervisión clara y adecuada por parte de las autoridades de control, lo que significa que no siempre cumplen con los requisitos de protección de datos exigidos por la ley, esta falta de regulación eficaz permite que los datos personales de los ciudadanos se almacenen y manipulen sin que los individuos sepan quién tiene acceso a esta información, cómo se usa o si pueden rectificarla en caso de que sea incorrecta, la desprotección de los ciudadanos ante estos servicios implica una vulneración directa a la garantía constitucional del habeas data.

Existe el riesgo de que Dataservice vendan o intercambien información personal con terceros sin el consentimiento de los titulares de los datos, en muchos casos, estos datos se utilizan para fines comerciales, segmentación de mercado o hasta con propósitos de vigilancia, esto deja a los ciudadanos ecuatorianos en una situación de vulnerabilidad, ya que no solo pierden

el control sobre su información, sino que también podrían verse expuestos a campañas de marketing invasivas, discriminación o decisiones automatizadas que afecten sus derechos sin posibilidad de rectificación.

Otro aspecto preocupante es el acceso que pueden tener la plataforma de Dataservice a datos sensibles, como la información financiera, historial médico o antecedentes judiciales de los ciudadanos, cuando estas plataformas manejan información sensible sin los debidos protocolos de protección y sin que los ciudadanos puedan verificar o controlar este acceso, se produce una invasión a la privacidad que contradice los principios del habeas data, sobre el derecho al control sobre los datos personales en estos casos es fundamental, pues la exposición de estos datos puede causar graves daños personales y económicos.

Para mitigar el impacto de vulneración de datos en la página de Dataservice, es esencial que existan leyes más estrictas y mecanismos de control que obliguen a estas plataformas a informar adecuadamente a los ciudadanos sobre el uso de sus datos y a obtener su consentimiento, en este instancia las autoridades deben fortalecer los medios por los cuales los ciudadanos pueden ejercer su derecho sobre la garantía constitucional del habeas data, garantizando así la transparencia y la protección de sus datos personales, es claro que sin una regulación clara y estricta, el crecimiento de dataservice seguirá representando una amenaza para la privacidad y el control sobre la información personal en el país.

### **2.2.15 Tecnología de la información y comunicación (TIC)**

El hábeas data, aunque tradicionalmente se ha entendido como una garantía que permite acceder y conocer la información personal en poder de terceros, actualmente se considera una acción procesal-constitucional clave para proteger los derechos de los ciudadanos frente al tratamiento indebido de sus datos personales, esta acción está vinculada a los derechos conocidos como ARCO, que incluyen el Acceso, Rectificación, Cancelación y Oposición, estas facultades conforman el núcleo del derecho a la autodeterminación informativa o libertad informática, ya que permiten a los individuos ejercer control sobre el uso y tratamiento de su información personal.

Dentro de la garantía jurisdiccional Enrique Pérez (2017) menciona que el hábeas data ofrece protección constitucional frente al impacto de las nuevas tecnologías de la información y comunicación para fundamentar esta propuesta, se utilizó una metodología basada en una investigación documental de carácter descriptivo, el objetivo se centró en analizar el marco legal de Ecuador respecto al hábeas data y en identificar los elementos jurídicos necesarios para garantizar su aplicación en la sociedad de la información. dado que el hábeas data y el derecho a la autodeterminación informativa son herramientas que protegen otros derechos fundamentales, en el contexto de la sociedad de la información no se busca prohibir el uso de las TIC, sino armonizarlas con el respeto a la dignidad humana, los resultados de esta investigación destacan la importancia de las resoluciones de la Corte Constitucional en este ámbito, así, la libertad informática y la autodeterminación informativa emergen como instituciones jurídicas que no solo protegen el acceso a la información personal, sino también el control sobre su uso frente a las tecnologías de la información y comunicación.

Esta acción tiene como objetivo permitir a las personas conocer, acceder, rectificar, eliminar y prohibir la divulgación de ciertos datos, ya sea porque fueron tratados de forma indebida o porque se intenta utilizarlos o compartirlos para fines distintos a los que justificaron su recopilación, así se busca prevenir que mediante el cruce ilegal de bases de datos, se elaboren "perfiles de personalidad" que puedan generar evaluaciones discriminatorias o incorrectas, evitando así posibles perjuicios para la persona a la que corresponden dichos datos.

#### **2.2.16 Deficiencia de aplicación uniforme de principios de protección de datos.**

La deficiencia en la aplicación uniforme de los principios de protección de datos personales es un problema recurrente que afecta gravemente la privacidad de los individuos y la efectividad de herramientas como el hábeas data, aunque en muchas jurisdicciones se han adoptado leyes específicas para regular el tratamiento de datos personales, la implementación de estos principios no siempre se realiza de manera consistente, esta falta de uniformidad genera incertidumbre y deja a los ciudadanos en una posición vulnerable, ya que las entidades públicas y privadas pueden no aplicar los estándares de protección de forma adecuada. El hábeas data, como mecanismo procesal constitucional, surge precisamente para

subsana estas deficiencias, permitiendo a las personas exigir el cumplimiento de los principios de protección de datos cuando consideran que sus derechos han sido vulnerados.

Uno de los problemas principales es la interpretación variada de los principios de protección de datos, como la transparencia, el consentimiento informado, la minimización de datos y la seguridad, dependiendo de la interpretación de los jueces o de las políticas internas de las entidades que manejan datos, los criterios aplicados pueden diferir significativamente. Esto se traduce en decisiones contradictorias al momento de resolver acciones de hábeas data, donde en algunos casos se concede acceso a los datos o se ordena su corrección, mientras que en otros se niega dicha solicitud, la falta de un enfoque uniforme no solo afecta la efectividad del hábeas data, sino que también socava la confianza en el sistema de justicia y en los mecanismos de protección de datos.

Además, la ausencia de lineamientos claros para la aplicación del hábeas data en relación con los principios de protección de datos ha generado un entorno de inseguridad jurídica, aunque existe un marco normativo que regula el uso de datos personales, la implementación de los principios sigue siendo desigual. Por ejemplo, la rectificación y eliminación de datos incorrectos, elementos fundamentales del hábeas data, a menudo enfrentan obstáculos burocráticos y interpretativos que limitan su eficacia. Las entidades responsables del tratamiento de datos suelen adoptar medidas reactivas en lugar de proactivas, atendiendo las solicitudes solo cuando los ciudadanos inician acciones legales, en lugar de garantizar de manera continua el cumplimiento de los principios de protección.

## **2.2 Marco Legal**

### **2.2.1 Constitución de la República del Ecuador**

Tras la disolución de la Gran Colombia, Ecuador declaró su independencia y promulgó su primera Constitución en 1830, instaurando un régimen republicano influido por las ideas liberales de la época, a lo largo del siglo XIX, el país experimentó varios cambios políticos que llevaron a la creación de varias constituciones, como las de 1843, 1851 y 1861, que reflejaron la disputa entre facciones conservadoras y liberales, así como las modificaciones en la estructura del Estado.

En el siglo XX, la Constitución de 1945 fue relevante por su intento de modernizar el sistema político, con un enfoque más democrático y una ampliación de los derechos políticos. Sin embargo, fue derogada en 1946 debido a la inestabilidad política de la época, la Constitución aprobada durante el gobierno de Jamil Mahuad se enfocó en los derechos humanos y el desarrollo sostenible, además de incluir principios sobre equidad de género y los derechos de los pueblos indígenas, y promover la descentralización del poder.

La actual Constitución, aprobada en 2008 mediante referéndum durante la administración de Rafael Correa, se caracteriza por ser plurinacional y por establecer un marco jurídico basado en el "buen vivir" también reconoce los derechos de la naturaleza y fortalece la participación ciudadana, los derechos sociales, y el control estatal sobre sectores estratégicos.

Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Establece un principio fundamental relacionado con el derecho de acceso a la información personal, tanto en el ámbito público como privado, este derecho garantiza que cualquier persona, por su propia iniciativa o a través de un representante legal, puede conocer si existe información sobre sí misma en bases de datos, documentos o archivos, independientemente de si están almacenados en formato físico o electrónico, el derecho a acceder a esta información se extiende también a la posibilidad de conocer qué tipo de datos se recopilan, el uso que se les da, su procedencia, a quién se destinan y por cuánto tiempo serán conservados.

Este derecho es clave dentro del marco de la protección de datos personales, ya que permite a los individuos ejercer control sobre su información personal y exigir la corrección o eliminación de datos inexactos, incompletos o que se utilicen de manera indebida, el hecho de que el texto incluya tanto a entidades públicas como privadas resalta la amplitud de su alcance, lo que refuerza la protección de los derechos de privacidad en diversos contextos,

como en servicios comerciales, instituciones gubernamentales, empresas tecnológicas, entre otros.

No solo garantiza el acceso, sino también la transparencia en el uso de los datos, al permitir a las personas conocer la finalidad del tratamiento de su información y su tiempo de almacenamiento, se promueve la rendición de cuentas por parte de las entidades que manejan datos, esto también está alineado con el principio de minimización de datos, que estipula que los datos personales no deben conservarse por más tiempo del necesario. En cualquier caso, no se protegen los datos en sí mismos, sino a los titulares de esos datos que consiste en la libertad de un titular respecto de cómo disponer de sus datos personales, es decir, no solo aquellos referidos al ámbito de su intimidad o privacidad, sino incluso los no autorizados, equivocadas o inexactas, en consecuencia, debe atribuirse mayores niveles y garantías de protección y accesibilidad a los datos personales, es conveniente insistir en que la accesibilidad de datos personales, es también un instituto de garantía de otros derechos fundamentales, ya que la influencia y repercusión de la recopilación, tratamiento y difusión de los datos personales afectan directamente el ejercicio de las libertades individuales en una sociedad en la que lo virtual y lo real se interrelacionan constantemente.

Art. 66.- Se reconoce y garantizará a las personas:

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

El artículo 66, numeral 19 de la Constitución de Ecuador establece el derecho a la protección de los datos personales como un derecho fundamental de los ciudadanos, este precepto reconoce la importancia de que las personas tengan control sobre su información personal, garantizando tanto el acceso a dichos datos como la capacidad de decidir cómo se utilizarán. Este derecho no solo abarca la protección frente a accesos no autorizados, sino también la facultad de las personas para determinar quién puede recolectar, procesar, archivar, distribuir o difundir su información personal.

Este derecho es crucial en la era digital, donde la circulación de datos personales es constante y masiva, debido al uso generalizado de internet, redes sociales, servicios en línea y tecnologías emergentes, la protección de los datos personales adquiere así una relevancia especial, ya que la vulneración de este derecho puede tener consecuencias graves, como la pérdida de privacidad, robo de identidad, discriminación o explotación comercial sin consentimiento.

El consentimiento del titular es un principio central en esta norma, ya que ninguna recolección, procesamiento o difusión de datos personales puede realizarse sin la autorización explícita de la persona afectada, salvo en aquellos casos donde la ley lo permita expresamente, esto protege la autodeterminación informativa, que es el derecho de las personas a decidir sobre el uso de su información, en situaciones en las que la ley autorice el acceso a los datos sin el consentimiento del titular, como en el marco de investigaciones judiciales, este acceso debe estar estrictamente regulado para evitar abusos y proteger los derechos fundamentales.

Otro punto clave es la regulación de la recolección y archivo de los datos personales. Esta norma prevé que cualquier proceso de recolección y almacenamiento de datos debe cumplir con estándares de seguridad y legalidad, esto es relevante en el ámbito de las empresas y organismos que manejan grandes volúmenes de datos personales, como bancos, empresas tecnológicas, hospitales, etc., estos actores tienen la obligación de asegurar que los datos sean tratados de manera adecuada y segura, protegiéndolos de accesos no autorizados o filtraciones.

La distribución y difusión de los datos personales también está sujeta a autorización, lo que implica que ninguna entidad o persona puede compartir datos sin el consentimiento expreso del titular, esto es especialmente relevante en contextos donde la información puede ser utilizada para fines comerciales, políticos o incluso delictivos, en un entorno donde el tráfico de datos personales puede generar enormes ganancias, este principio protege a los ciudadanos de posibles abusos.

Este artículo promueve un equilibrio entre el uso legítimo de los datos personales y la protección de la intimidad de los individuos, la norma constitucional busca salvaguardar los derechos de los ciudadanos frente a los riesgos asociados a la explotación indebida de sus datos, promoviendo un ambiente de mayor seguridad y transparencia en el manejo de la información.

### **2.2.2 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional**

Esta ley, aprobada en 2009, fue una respuesta directa a la necesidad de implementar las disposiciones de la Constitución de 2008, la cual promovió un marco más inclusivo y participativo para la defensa de los derechos fundamentales, la LOGJCC se convirtió en un instrumento esencial para establecer los mecanismos necesarios para la protección de los derechos establecidos en la nueva constitución, se caracteriza por varios periodos de inestabilidad política y jurídica en Ecuador, especialmente en las décadas de los 90 y principios del 2000. Durante estos años, el país experimentó una serie de crisis institucionales, con cambios frecuentes en el gobierno, inestabilidad económica y demandas sociales que no lograban ser atendidas de manera efectiva por el Estado, el sistema de justicia constitucional en ese entonces era débil, y no existían mecanismos sólidos para garantizar la protección de los derechos humanos, esta situación generó una creciente demanda por parte de la sociedad civil y de sectores políticos para fortalecer el control constitucional y las garantías jurisdiccionales.

La reforma constitucional de 2008 marcó un punto de inflexión en la historia del derecho en Ecuador, esta Constitución, resultado de un proceso constituyente con amplia participación popular que consagró un modelo de Estado plurinacional y garantista, en el que se reconocen no solo los derechos individuales, sino también derechos colectivos, ambientales y de la naturaleza, la creación de una ley que regulase el acceso a las garantías jurisdiccionales y el control constitucional se volvió una prioridad para hacer efectiva la protección de estos derechos, surgió como un instrumento jurídico clave para implementar estos principios constitucionales.



La historia de la LOGJCC fue la creación de la Corte Constitucional del Ecuador, antes de la Constitución de 2008, el control constitucional estaba fragmentado y no existía una institución fuerte dedicada exclusivamente a este fin, con la creación de la Corte Constitucional en la nueva carta magna, se estableció la necesidad de un marco normativo que regulara sus competencias, atribuciones y el procedimiento para la protección de los derechos constitucionales, lo que se consolidó con la aprobación en 2009. esta ley definió los mecanismos de acción como el hábeas corpus, el hábeas data, la acción de protección, entre otros.

En términos regionales, también se inscribe en el contexto más amplio de las reformas constitucionales que tuvieron lugar en América Latina durante las primeras décadas del siglo XXI. Países como Colombia y Bolivia también implementaron reformas orientadas a fortalecer el control constitucional y los mecanismos de protección de derechos. En particular, Ecuador tomó como referencia el modelo de tutela colombiano, que ya había demostrado ser un mecanismo eficaz para la defensa rápida y efectiva de los derechos fundamentales, el desarrollo también estuvo influenciado por los estándares internacionales de derechos humanos. Organismos como la Corte Interamericana de Derechos Humanos y la Comisión Interamericana de Derechos Humanos han jugado un papel relevante en la promoción de mecanismos de control constitucional efectivos en los países miembros. Ecuador, al ser signatario de tratados internacionales en materia de derechos humanos, debía cumplir con ciertas obligaciones internacionales, al establecer mecanismos de protección de los derechos y el control de la constitucionalidad, también responde a las exigencias y recomendaciones de estos organismos internacionales para garantizar el acceso a la justicia y la protección de los derechos humanos en el país.

Art. 49.- Objeto. - La acción de hábeas data tiene por objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos.

Establece la acción de hábeas data como un mecanismo legal para garantizar el acceso y control sobre los datos personales que entidades públicas o privadas posean sobre una

persona. Esta acción responde a la creciente importancia de la protección de datos en un mundo donde la información personal puede ser recolectada, almacenada y procesada de diversas maneras, muchas veces sin el conocimiento o consentimiento explícito de los individuos, el objetivo primordial del hábeas data es asegurar que las personas puedan conocer, actualizar o eliminar información que les concierne, evitando abusos en el manejo de sus datos personales.

El artículo no solo protege el derecho al acceso a los datos, sino también a saber cómo y por qué se utiliza esta información, esto incluye aspectos como la finalidad de su uso, el origen de los datos y el tiempo que estarán vigentes en archivos o bancos de datos. Este nivel de transparencia y control es fundamental en un contexto donde la información personal es cada vez más valiosa y vulnerable a malos usos. Por ejemplo, en casos de discriminación, manipulación o fraude, las personas tienen una herramienta legal para defender sus derechos frente a entidades que puedan estar utilizando indebidamente su información.

Otro aspecto importante de este artículo es que extiende el ámbito de protección del hábeas data a datos almacenados en soportes materiales o electrónicos, lo que refleja una visión moderna y actualizada del manejo de la información en la era digital, esto incluye desde bases de datos físicos en entidades públicas hasta información almacenada en sistemas electrónicos o en la nube por empresas privadas, la inclusión de estos formatos amplía el alcance de la acción, reconociendo que el tratamiento de datos hoy no se limita a documentos en papel, sino que también abarca archivos digitales, redes sociales, bases de datos en línea y otros medios electrónicos. Finalmente, el artículo reconoce el derecho de las personas a cuestionar y pedir la rectificación de los datos inexactos o falsos que les afecten. Esta disposición es esencial para evitar daños que puedan derivarse de información incorrecta en bases de datos.

Art. 50.- **Ámbito de protección.** - Se podrá interponer la acción de hábeas data en los siguientes casos: 1. Cuando se niega el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o estén en poder de personas naturales o jurídicas privadas. 2. Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos. 3. Cuando se da un uso de la información personal que viole un

derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente.

El Artículo 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional establece el ámbito de protección del hábeas data, definiendo los casos específicos en los que una persona puede interponer esta acción, el primer caso señalado es cuando se niega el acceso a los datos personales que estén en poder de entidades públicas o privadas, este aspecto garantiza que las personas no solo tienen el derecho a que sus datos sean gestionados de manera correcta, sino también a acceder a ellos para verificar su exactitud y el uso que se les da, la negativa de acceso representa una vulneración directa a la transparencia y al control que un individuo debe tener sobre su propia información.

El segundo punto establece que el hábeas data también puede interponerse cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos, este apartado resulta clave para la protección de derechos, ya que reconoce que los datos personales incorrectos o desactualizados pueden tener un impacto negativo en la vida de las personas, afectando su reputación, integridad o derechos patrimoniales, la capacidad de rectificar o eliminar información incorrecta permite a los individuos ejercer control sobre los errores que puedan perjudicarles y evita que continúen circulando datos inexactos que puedan causarles daño.

El tercer punto se refiere a la utilización indebida de los datos personales sin autorización expresa, excepto en los casos en que exista una orden judicial competente, esto protege a las personas frente a la manipulación, venta o uso inapropiado de su información por parte de terceros, una preocupación creciente en la era digital, la información personal, como los datos financieros, médicos o incluso de comportamiento, puede ser explotada para fines comerciales o de vigilancia sin el conocimiento de los individuos, y este apartado busca prevenir tales abusos al garantizar que solo se pueda utilizar con consentimiento o bajo el amparo de la ley.

El reconocimiento de estas situaciones como vulneraciones de derechos constitucionales fortalece el marco jurídico para la protección de la privacidad y los derechos de los individuos, subrayando el rol del Estado en garantizar un manejo ético y transparente de la

información personal, esto es especialmente relevante en un mundo donde los datos personales se han convertido en un recurso valioso, y su mal manejo puede tener repercusiones graves en la vida de las personas.

### **2.2.3 Ley orgánica de protección de datos personales**

En mayo de 2021, surge como respuesta a la creciente necesidad de regular el uso y manejo de datos personales en un entorno cada vez más digitalizado, antes de esta ley, el país carecía de una normativa específica y robusta en la materia, lo que dejaba un vacío legal significativo frente a la protección de la privacidad y el manejo de la información de los ciudadanos, la Constitución de 2008 ya reconocía el derecho a la protección de datos personales, pero faltaba una ley que estableciera los mecanismos específicos para garantizarlo.

El desarrollo de esta ley también fue influenciado por normativas internacionales, en especial el Reglamento General de Protección de Datos de la Unión Europea, que se ha convertido en un referente global en cuanto a la regulación del tratamiento de datos, el crecimiento exponencial del uso de internet, redes sociales, y la adopción de tecnologías que recolectan grandes volúmenes de datos personales, como las aplicaciones móviles y servicios en la nube, aceleró la demanda de un marco legal que regulara el tratamiento adecuado de dicha información y brindara protección efectiva frente a abusos o violaciones.

Esta ley establece principios claves como el consentimiento informado, la finalidad legítima del uso de los datos, y el derecho de acceso, rectificación y eliminación de los datos por parte de los titulares, además, crea la Autoridad Nacional de Protección de Datos Personales, encargada de velar por el cumplimiento de la ley y sancionar las infracciones, en esencia, la ley se alinea con las tendencias globales hacia una mayor protección de la privacidad y la seguridad de los datos, respondiendo a las exigencias de un entorno tecnológico moderno y a las demandas de los ciudadanos por un mayor control sobre su información personal.

Art. 1.-Objeto y finalidad. -El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

El Artículo 1 de la Ley Orgánica de Protección de Datos Personales de Ecuador establece como su objetivo central la garantía del derecho a la protección de datos personales, este derecho incluye tanto el acceso como la decisión sobre la información personal, lo que implica que los titulares de los datos tienen el control sobre cómo se recopila, utiliza, almacena y difunde su información, esta disposición es crucial en el contexto moderno, donde el uso y tratamiento de datos personales son parte cotidiana de actividades comerciales, tecnológicas y sociales.

El artículo también subraya que, para cumplir con este objetivo, la ley regula y desarrolla un conjunto de principios, derechos, obligaciones y mecanismos de tutela, entre los principios se encuentran los de legalidad, transparencia, confidencialidad y proporcionalidad, los cuales orientan el tratamiento adecuado de los datos personales, la legalidad implica que el manejo de los datos debe estar amparado por una norma jurídica o el consentimiento expreso del titular, mientras que la transparencia asegura que las personas sepan cómo y por qué se usan sus datos, la confidencialidad garantiza que la información personal sea protegida contra accesos no autorizados y, finalmente, la proporcionalidad limita el uso de datos a lo estrictamente necesario para la finalidad que se ha informado.

Además, señala que la ley también desarrolla derechos y obligaciones, los derechos incluyen, entre otros, el derecho de acceso a los propios datos, el derecho de rectificación si estos son inexactos y el derecho al olvido, que permite la eliminación de la información cuando ya no sea relevante o necesaria para el fin con el que fue recopilada, por otro lado, las obligaciones recaen principalmente en quienes manejan los datos, quienes deben cumplir con medidas de seguridad, notificar a los titulares sobre el uso de sus datos, y obtener el consentimiento informado antes de cualquier procesamiento, estas obligaciones buscan proteger a las personas de la explotación o uso indebido de su información personal, especialmente en contextos donde las tecnologías facilitan la manipulación de grandes volúmenes de datos.

Finalmente, menciona los mecanismos de tutela, que permiten a los titulares de los datos exigir el respeto de sus derechos y presentar reclamaciones en caso de vulneraciones, estos mecanismos incluyen recursos administrativos y judiciales que aseguran que el derecho a la protección de datos sea efectivamente resguardado, además, la ley establece la creación de

una Autoridad Nacional de Protección de Datos, que tendrá la tarea de supervisar el cumplimiento de la normativa, sancionar infracciones y promover la educación sobre los derechos en esta materia.

#### **2.2.4 Ley de comercio electrónico, firmas y mensajes de datos**

En el año 2002 como parte de un esfuerzo por regular el creciente uso de las tecnologías digitales en el ámbito comercial, antes de esta ley, el país carecía de un marco normativo que reconociera formalmente las transacciones realizadas de forma electrónica, lo que generaba inseguridad jurídica y falta de confianza entre los usuarios y las empresas, el rápido avance del internet y la digitalización de las comunicaciones hicieron necesaria una normativa que garantizara la validez y legalidad de los documentos y contratos firmados electrónicamente.

Uno de los antecedentes más importantes fue la Ley Modelo de la UNCITRAL sobre Comercio Electrónico de 1996, la cual sirvió como base para varias legislaciones en América Latina, incluyendo la de Ecuador, este modelo proporcionó directrices sobre cómo integrar las tecnologías de la información en el comercio, asegurando que las transacciones digitales tuvieran el mismo reconocimiento legal que las realizadas en papel, la legislación ecuatoriana adaptó estos principios a su contexto, introduciendo disposiciones que regulan el uso de firmas electrónicas y mensajes de datos para garantizar su integridad, autenticidad y no repudio.

La ley también sentó las bases para promover el comercio electrónico en Ecuador, incentivando la adopción de tecnologías digitales tanto por parte de empresas como del sector público, además, estableció la infraestructura jurídica y tecnológica para el uso de certificados digitales y autoridades certificadoras, esenciales para garantizar la seguridad de las transacciones en línea, con esta normativa, Ecuador buscaba modernizar su sistema comercial y fomentar la confianza en las transacciones digitales, marcando un paso importante hacia la digitalización y el desarrollo de una economía más conectada.

Art. 9.- Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

Establece un principio fundamental en la protección de datos personales al exigir el consentimiento expreso del titular para la elaboración, transferencia o utilización de bases de datos que contengan información obtenida de mensajes de datos, este requerimiento de consentimiento refuerza la idea de que los individuos tienen el derecho de controlar cómo se utiliza su información personal, alineándose con las mejores prácticas internacionales en materia de protección de datos.

La exigencia del consentimiento expreso implica que los titulares de datos deben ser informados de manera clara y comprensible sobre el uso que se dará a su información. Este enfoque garantiza que los individuos no solo sean conscientes de la recopilación de sus datos, sino que también tengan la opción de aceptar o rechazar dicha recopilación, este principio es esencial para construir una relación de confianza entre las organizaciones que manejan datos y los consumidores, ya que el uso irresponsable de la información puede llevar a violaciones de privacidad y daños a la reputación de las personas.

Además, menciona que el titular de los datos puede seleccionar la información a compartirse con terceros, lo que resalta el derecho a la autodeterminación informativa, este derecho permite a los individuos decidir qué datos específicos quieren que se compartan y con quién, evitando así la divulgación de información sensible o irrelevante, esto es especialmente importante en un contexto donde las bases de datos a menudo contienen información personal que puede ser utilizada para fines comerciales, de marketing o incluso delictivos.

También refleja la necesidad de establecer límites claros en el manejo de datos personales en la era digital, la recopilación de datos debe ser proporcional a la finalidad para la que se utilizan, evitando prácticas abusivas como el uso excesivo de información personal o la venta de datos sin el consentimiento del titular, este enfoque no solo protege la privacidad individual, sino que también ayuda a regular el comportamiento de las empresas y organizaciones que manejan grandes volúmenes de información.

La protección de datos también implica un compromiso por parte de las empresas para implementar medidas adecuadas de seguridad en el manejo de la información, las organizaciones deben asegurarse de que los datos sean tratados de manera segura y que

existan protocolos claros para la obtención de consentimientos, así como para la gestión de solicitudes de acceso, rectificación o eliminación de datos, esto no solo es un requisito legal, sino que también contribuye a la reputación y la confianza del cliente, un marco claro para la protección de datos personales en el contexto del comercio electrónico, enfatizando la importancia del consentimiento y la autodeterminación del titular de los datos, esta normativa no solo protege los derechos de los individuos, sino que también fomenta un entorno más seguro y responsable en el uso de tecnologías digitales, la implementación efectiva de estos principios es crucial para promover una cultura de respeto a la privacidad en el ámbito comercial y digital, a medida que la tecnología continúa avanzando y transformando las interacciones humanas y comerciales.

### **2.2.5 Constitución de la República de Argentina**

El 1 de mayo de 1853, marcando un hito fundamental en la historia política y jurídica del país, antes de esta constitución, Argentina atravesó un período de conflictos y luchas internas que dificultaron la unificación y estabilidad del territorio, durante las décadas previas, las provincias argentinas operaban de manera autónoma y a menudo estaban involucradas en disputas entre facciones, lo que llevó a la necesidad de establecer un marco legal que garantizara la organización del Estado y la protección de los derechos de los ciudadanos, la constitución fue resultado de un consenso alcanzado en la Convención Constituyente de Santa Fe, donde representantes de varias provincias discutieron y acordaron los principios fundamentales que regirían la nación. Uno de los principales antecedentes de la Constitución argentina fue la Constitución de 1819, que había sido un intento inicial de establecer un marco constitucional, pero no logró ser efectiva debido a la falta de consenso entre las provincias y el contexto de guerras civiles que asolaban el país.

Posteriormente, el Pacto Federal de 1831 fue un acuerdo importante entre las provincias, pero aún carecía de un marco constitucional formal, la necesidad de una constitución se hizo evidente tras el establecimiento de la Confederación Argentina bajo el liderazgo de Juan Bautista Alberdi, quien fue un fuerte defensor de la creación de una constitución que integrara y diera coherencia al país.



La Constitución de 1853 se inspiró en diversas corrientes de pensamiento político y jurídico de la época, incluyendo influencias del liberalismo y el republicanism, tomó elementos de la Constitución de los Estados Unidos y otras constituciones de Europa y América Latina, adaptándolos al contexto argentino, la norma establece principios fundamentales, como la división de poderes, el federalismo, la protección de los derechos individuales y la promoción del bienestar general, a lo largo de los años, la Constitución ha sido reformada en varias ocasiones, siendo la más significativa en 1949, que introdujo nuevos derechos sociales y económicos, reflejando las demandas de una sociedad en constante evolución, la Constitución argentina ha sido un pilar en la construcción del Estado y en la garantía de los derechos de los ciudadanos, constituyendo un referente en la legislación latinoamericana.

Artículo 43.- Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley.

Establece un mecanismo de defensa constitucional conocido como acción de amparo, que tiene como objetivo proteger de manera rápida y expedita los derechos fundamentales de las personas cuando estos son vulnerados o amenazados por acciones u omisiones arbitrarias o ilegales, ya sea por parte de autoridades o de particulares, este recurso es esencial dentro del sistema judicial argentino, ya que permite a cualquier persona acudir a la justicia cuando sus derechos son lesionados de forma actual o inminente, garantizando una respuesta judicial inmediata ante la falta de otros medios más idóneos.

El amparo tiene características fundamentales que lo hacen un recurso eficaz y directo para la protección de los derechos, su celeridad se destaca al requerir que el proceso sea rápido y que la persona afectada pueda obtener una solución urgente, evitando así demoras prolongadas que podrían agravar el perjuicio, deja claro que esta acción solo puede interponerse cuando no exista otro medio judicial más adecuado, lo que asegura que el amparo no se convierta en un recurso de uso indiscriminado o que sustituya a otros procedimientos judiciales que pudieran ser más específicos o efectivos.

Este mecanismo protege una amplia gama de derechos y garantías reconocidos no solo por la Constitución, sino también por tratados internacionales y leyes, esto incluye derechos individuales, como la libertad, la vida, la integridad física y los derechos sociales, entre otros. Además, el amparo puede ser invocado tanto frente a actos que ya han causado un daño como ante situaciones que representan una amenaza inminente de vulneración de derechos, lo que lo convierte en un instrumento preventivo y correctivo, el concepto de ilegalidad manifiesta o arbitrariedad es clave, ya que implica que el acto u omisión cuestionado debe estar claramente fuera del marco legal o ser claramente injusto, proporcionando un límite a los casos en los que se puede utilizar el amparo.

Este artículo también es notable por permitir que el amparo sea interpuesto no solo contra el Estado, sino también contra particulares, esto es crucial en un contexto donde las violaciones de derechos no siempre provienen del poder público, sino también de actores privados, como empresas o individuos, lo que amplía el ámbito de protección de los derechos constitucionales, además, se complementa con otras herramientas judiciales, como el hábeas corpus y el hábeas data, que refuerzan la defensa de derechos específicos.

El Artículo 43 garantiza un acceso efectivo y rápido a la justicia en casos de violación o amenaza de derechos fundamentales, ofreciendo a las personas una vía de protección inmediata cuando no existen otros medios judiciales más idóneos, su implementación fortalece el sistema de garantías constitucionales en Argentina, protegiendo a los ciudadanos frente a arbitrariedades e ilegalidades tanto del Estado como de actores privados.

#### **2.2.6 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional de Argentina**

En Argentina no existe una ley orgánica específica de garantías jurisdiccionales y control constitucional para el hábeas data debido a que la protección de esta garantía se encuentra regulada en diversos cuerpos normativos que permiten su ejercicio sin la necesidad de una ley concentrada en su totalidad.

El hábeas data está consagrado en la Constitución Nacional (artículo 43) la cual establece los mecanismos para que cualquier persona pueda solicitar el acceso, actualización o

eliminación de sus datos personales, este sistema descentralizado permite que los tribunales, en base a las normativas ya existentes, ejerzan el control constitucional de forma efectiva sin la creación de una ley orgánica única para estos casos.

### **2.2.7 Ley de Acceso a la Información - Ley 27.275**

En 2016, tiene como principal antecedente la necesidad de fortalecer la transparencia y el control ciudadano sobre la administración, antes de esta ley, Argentina carecía de una normativa integral y moderna que regulara el acceso a la información, lo que limitaba la posibilidad de los ciudadanos de ejercer un control efectivo sobre los actos del gobierno, a lo largo de los años, organizaciones de la sociedad civil y organismos internacionales como la Organización de Estados Americanos (OEA) y la Organización de las Naciones Unidas (ONU) promovieron el establecimiento de marcos jurídicos que garantizaran este derecho fundamental.

En el plano internacional, la Convención Interamericana contra la Corrupción y la Declaración de Principios sobre Libertad de Expresión de la Comisión Interamericana de Derechos Humanos fueron influyentes para impulsar leyes de acceso a la información en América Latina, a nivel local, antes de la sanción de la Ley 27.275, algunas provincias y municipios argentinos ya habían implementado normativas sobre transparencia, pero estas eran insuficientes o dispares en su aplicación, de hecho, el decreto 1172/2003, dictado durante el gobierno de Néstor Kirchner, fue un antecedente importante a nivel nacional, aunque su alcance estaba limitado solo al Poder Ejecutivo.

La Ley 27.275 estableció un marco integral para garantizar que todas las personas tengan el derecho de acceder a la información en poder de organismos públicos, organismos no estatales que reciben fondos públicos y empresas del Estado, la norma establece principios clave como la transparencia, la presunción de publicidad de la información y la celeridad en los plazos de respuesta, además, la ley creó la Agencia de Acceso a la Información, encargada de garantizar el cumplimiento de la normativa y promover una cultura de transparencia, esta ley fue un paso importante en la democratización de la información y el fortalecimiento de la rendición de cuentas en Argentina.

Artículo 33. - (Procedencia). 1. La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

Establece las condiciones bajo las cuales procede la acción de protección de datos personales o hábeas data en Argentina, lo que constituye un mecanismo fundamental para garantizar el derecho de los ciudadanos a conocer y controlar la información que sobre ellos se encuentra almacenada en bases de datos públicos o privados, contempla dos situaciones clave en las que los ciudadanos pueden ejercer esta acción: el acceso a la información almacenada y la corrección de datos incorrectos o prohibidos por la ley.

El primer punto de la norma establece que cualquier persona puede solicitar acceso a los datos personales almacenados en archivos, registros o bases de datos, independientemente de si son de naturaleza pública o privada, siempre que estos tengan como finalidad la provisión de informes, esto asegura el derecho de acceso a la información personal y garantiza la transparencia en el tratamiento de datos, permitiendo que los ciudadanos conozcan qué información se almacena sobre ellos, cómo se utiliza, y con qué propósito, este derecho es crucial en un contexto donde la digitalización y el uso masivo de datos han aumentado, ya que muchas veces los individuos no tienen claro el tipo de información que las entidades almacenan sobre ellos.

El segundo punto del artículo se refiere a los casos en que la información almacenada sea falsa, inexacta, desactualizada o tratada de manera ilegal, en estos casos, el titular de los datos puede exigir su rectificación, actualización, supresión o confidencialidad, dependiendo de la situación, esto significa que la persona no solo tiene derecho a acceder a sus datos, sino también a corregir o eliminar cualquier dato que no refleje la verdad o que haya sido obtenido o tratado de manera incorrecta, el derecho a la supresión de datos es particularmente importante cuando se trata de información sensible que podría dañar la privacidad o los derechos de una persona si no se maneja adecuadamente.

Además, el artículo contempla la posibilidad de exigir la supresión o confidencialidad de los datos cuando el registro de estos esté prohibido por la ley, esto asegura que las entidades no puedan recopilar o almacenar información que esté fuera de los límites legales, protegiendo así los derechos de los ciudadanos y evitando posibles abusos en el manejo de datos sensibles, como información relacionada con la raza, religión, orientación sexual o preferencias políticas, cuya recopilación sin consentimiento explícito está prohibida por la ley, esta disposición refuerza el principio de autodeterminación informativa, que garantiza que cada persona tenga control sobre sus propios datos y decida qué información puede o no ser almacenada o utilizada por terceros.

Es una pieza clave en la protección de la privacidad y los derechos individuales en Argentina, ya que no solo permite a las personas acceder a su información personal, sino que también les otorga el poder de corregir o eliminar datos incorrectos o no autorizados. Este derecho refuerza el marco legal que regula el tratamiento de datos personales en un mundo cada vez más digitalizado, protegiendo a los ciudadanos contra la desinformación, la manipulación de datos y el uso indebido de su información personal.

Artículo 34. - (Legitimación activa). La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.

En la acción de hábeas data, es decir, quiénes están facultados para ejercer este derecho y presentar una demanda de protección de datos, el artículo es crucial porque establece quién puede invocar esta acción judicial, tanto en nombre propio como en representación de otras personas y cómo intervienen los representantes legales en el caso de personas jurídicas o incapaces, se establece que la acción de hábeas data puede ser ejercida por el afectado directamente, lo que significa que cualquier persona cuyos datos personales sean almacenados o tratados puede solicitar la protección de su información. Este derecho personalísimo refuerza la autodeterminación informativa, dándole a cada individuo la capacidad de controlar y gestionar sus propios datos frente a terceros, además, este derecho no solo se circunscribe a la información errónea o desactualizada, sino también a la

protección frente a un tratamiento indebido de la información personal, lo que es esencial en un entorno de constante uso y almacenamiento de datos, También extiende la legitimación a los tutores, curadores y sucesores de las personas físicas. Esta disposición es importante porque asegura la protección de los datos personales en caso de que el titular de los datos no pueda actuar por sí mismo, ya sea por incapacidad o fallecimiento, los sucesores en línea directa o colateral hasta el segundo grado (hijos, padres, hermanos, etc.) pueden también accionar en representación del titular, lo que protege los derechos de privacidad de las personas incluso después de su muerte. Este aspecto es relevante, por ejemplo, para evitar que los datos de una persona fallecida sean utilizados de manera inapropiada o sin el debido consentimiento.

En cuanto a las personas jurídicas o personas de existencia ideal, el artículo aclara que la acción debe ser ejercida por sus representantes legales o apoderados designados, esto es fundamental, ya que las empresas o entidades también tienen derecho a la protección de los datos que les conciernen, sobre todo en relación con información sensible, comercial o confidencial. Las entidades jurídicas, al igual que las personas físicas, tienen la posibilidad de recurrir al hábeas data para acceder a la información que terceros que posean sobre ellas o para corregir datos que puedan perjudicar su imagen o funcionamiento.

Una característica notable de este artículo es la posibilidad de que el Defensor del Pueblo intervenga de manera coadyuvante en el proceso, esto significa que el Defensor del Pueblo puede actuar en apoyo del titular de los datos, reforzando la protección y el ejercicio de este derecho, el Defensor del Pueblo tiene la misión de velar por los derechos fundamentales y las garantías constitucionales de los ciudadanos y su intervención en estos procesos garantiza un mayor control y supervisión sobre el respeto a los derechos de privacidad y protección de datos, esto también implica que, en casos de especial relevancia o cuando el titular de los datos se encuentre en una situación de vulnerabilidad, el Defensor del Pueblo puede brindar un apoyo institucional que aumente la eficacia de la acción judicial.

Artículo 36. - (Competencia). Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor. Procederá la competencia federal: a) cuando se interponga en contra de archivos de datos públicos de organismos

nacionales, y b) cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales.

Establece las normas de competencia judicial para las acciones de hábeas data, especificando cuál es el juez que tiene la potestad para entender en estas causas, esta regulación es esencial para asegurar que los ciudadanos puedan ejercer su derecho a la protección de datos de manera efectiva y eficiente, al establecer un marco claro sobre dónde y ante quién pueden presentar sus reclamaciones.

Este artículo estipula que se procederá a la competencia federal en dos situaciones específicas, la primera es cuando se interponga una acción contra archivos de datos públicos de organismos nacionales, esta disposición es clave, ya que los organismos del Estado, al manejar información sensible y datos personales de ciudadanos, deben estar sujetos a un control judicial que garantice la transparencia y protección de estos derechos, la competencia federal asegura que haya un marco uniforme y coherente para el tratamiento de estos casos, evitando así discrepancias en la aplicación de la ley a nivel local.

La segunda situación que habilita la competencia federal se refiere a los archivos de datos que se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales, esta cláusula es especialmente relevante en un mundo cada vez más globalizado y digitalizado, donde los datos personales pueden circular entre diferentes jurisdicciones, al establecer la competencia federal en estos casos, se busca asegurar que haya un tratamiento adecuado y coherente de la información, y que los derechos de los ciudadanos sean protegidos en un contexto donde las barreras geográficas son difusas, esto es particularmente importante en situaciones en las que los datos se almacenan o procesan en servidores de distintos países, lo que plantea desafíos sobre cómo se deben manejar los datos personales y quién es responsable en caso de violaciones.

El Artículo 36 define de manera clara y precisa las reglas de competencia para las acciones de hábeas data, lo que permite a los ciudadanos ejercer su derecho de protección de datos de forma accesible y efectiva, al facilitar la elección del juez y establecer criterios para la competencia federal, la norma refuerza el marco jurídico que protege la privacidad de los ciudadanos y garantiza que los responsables del tratamiento de datos sean sujetos a un

control judicial efectivo, esta regulación es fundamental en un entorno en el que el manejo de datos personales está en constante evolución, y donde las interconexiones entre diferentes jurisdicciones demandan un enfoque coordinado y riguroso para salvaguardar los derechos individuales.

### **2.2.8 Ley orgánica de protección de datos- Ley 25.326**

La Ley 25.326, conocida como la Ley de Protección de los Datos Personales de Argentina, fue sancionada el 30 de octubre de 2000 y promulgada el 2 de noviembre de 2000, su objetivo principal es la protección integral de los datos personales almacenados en archivos, registros, bases de datos u otros medios técnicos, con el fin de garantizar el derecho a la privacidad de las personas, el desarrollo de la protección de datos personales está vinculado a la evolución tecnológica, particularmente en lo que respecta al uso de computadoras para almacenar y procesar información personal, los países europeos fueron pioneros en el desarrollo de leyes de protección de datos.

La inclusión del habeas data en la Constitución Nacional generó la necesidad de contar con una ley que reglamentara este derecho, el rápido avance de la tecnología y la creciente preocupación sobre el manejo de la información personal también impulsaron la creación de un marco normativo que garantizara la protección adecuada de los datos.

El proyecto de ley fue impulsado por el Poder Ejecutivo y discutido ampliamente en el Congreso de la Nación, para desarrollar una ley acorde a las nuevas demandas de protección de datos en el país, la Ley 25.326 fue sancionada y, en 2001, se creó la Dirección Nacional de Protección de Datos Personales como autoridad de control.

Con el tiempo, se ha considerado la necesidad de actualizar la Ley 25.326 debido a los avances tecnológicos y la aparición de nuevas normativas internacionales, como el Reglamento General de Protección de Datos (GDPR), que ha planteado un estándar más elevado para la protección de la privacidad y los datos personales.



Artículo 14.- (Derecho de acceso).

1. El titular de los datos, previa acreditación de su identidad tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.

2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.

Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.

3. El derecho de acceso a qué se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

El artículo 14 de la Ley 25.326 establece los derechos fundamentales de acceso a la información personal contenida en bases de datos, el titular de los datos tiene el derecho a conocer, en cualquier momento y sin costo alguno, la información que sobre él se encuentra almacenada en registros públicos o privado, este derecho de acceso es esencial para garantizar la transparencia en el tratamiento de los datos personales, lo que implica que cualquier persona puede requerir saber qué información suya ha sido recopilada, cómo se está utilizando y con qué fines.

El artículo también regula la posibilidad de que el titular de los datos pueda solicitar la corrección, actualización o, en su caso, la supresión de los datos si estos son incorrectos o están siendo utilizados de manera indebida, este derecho de rectificación es fundamental para proteger la privacidad y la integridad de la información personal, ya que garantiza que los datos almacenados sean precisos y reflejen la realidad, además, si los datos no están siendo tratados conforme a la ley, el titular puede exigir su eliminación, protegiendo así su derecho a la intimidad, refuerza la idea de control sobre la propia información personal, un principio central de la Ley 25.326, el ejercicio de estos derechos por parte de los ciudadanos es clave para prevenir abusos en el manejo de datos personales y establece un equilibrio entre el poder de las entidades que manejan datos y el derecho de las personas a mantener su privacidad.

Artículo 16. - (Derecho de rectificación, actualización o supresión).

1. Toda persona tiene derecho a que sean rectificadas, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.

El artículo 16 de la Ley 25.326 regula el derecho de supresión, rectificación, confidencialidad y almacenamiento de los datos personales, fortaleciendo la protección de los individuos frente al uso indebido o incorrecto de su información, este artículo establece que el titular de los datos puede exigir en cualquier momento la rectificación, actualización o supresión de la información que sea inexacta, incompleta o que esté siendo tratada de manera contraria a lo dispuesto por la ley, es un mecanismo clave para garantizar que la información almacenada sea precisa y utilizada dentro de los límites legales.

Además, contempla situaciones en las que la supresión de los datos no es procedente, como cuando existen obligaciones contractuales o legales que requieran su conservación, o cuando la información se utiliza para fines estadísticos, científicos o históricos, bajo condiciones de anonimato, estas excepciones demuestran que, aunque el derecho a la supresión es fundamental, existen ciertos límites necesarios para proteger otros intereses de carácter público o privado, lo que asegura un equilibrio entre la protección de los datos y otras necesidades legítimas.

Las entidades que recopilan, almacenan o procesan información personal tienen la obligación de asegurar que estos datos no sean accesibles a terceros no autorizados, y deben implementar las medidas de seguridad necesarias para proteger la información, el incumplimiento de estas disposiciones puede llevar a sanciones, subrayando la importancia de que el tratamiento de datos respete los principios de seguridad y confidencialidad establecidos por la ley.

### **2.2.9 Ley de comercio electrónico, firma y mensajes de datos**

En Argentina no existe una ley unificada de comercio electrónico, firmas electrónicas y mensajes de datos porque estos temas han sido regulados de manera dispersa a través de diversas leyes y decretos, en lugar de concentrarse en una única normativa integral, a falta de una ley específica de comercio electrónico refleja la evolución paulatina de este sector, que ha ido creciendo rápidamente con la tecnología, haciendo que las normas existentes se vayan complementando con regulaciones puntuales.

### **2.2.10 Constitución Política de Perú**

La Constitución Política del Perú de 1993, que fue modificada en 2005, es el resultado de un proceso histórico que busca establecer un marco jurídico fundamental para la organización del Estado y la garantía de derechos fundamentales, su promulgación se sitúa en un contexto de transición política tras la crisis económica y social que enfrentó el país en las décadas de 1980 y 1990, marcada por la hiperinflación, la violencia terrorista y la inestabilidad política. La necesidad de establecer un orden constitucional que promueva la democracia, el respeto a los derechos humanos y la estabilidad jurídica llevó a la convocatoria de una Asamblea Constituyente, que tuvo como objetivo elaborar una nueva carta magna que respondiera a las demandas sociales y políticas de la época, uno de los antecedentes más importantes en la creación de la Constitución de 1993 fue la Constitución de 1979, que fue la primera en el Perú en reconocer de manera expresa una serie de derechos sociales y económicos.

Sin embargo, esta constitución fue derogada en 1992 por un autogolpe de Estado del entonces presidente Alberto Fujimori, lo que llevó a la creación de un nuevo marco normativo, la Constitución de 1993, por lo tanto, refleja un intento de equilibrio entre el liberalismo económico y la necesidad de proteger los derechos fundamentales, incorporando principios de economía social de mercado y promoviendo la inversión privada como motor del desarrollo económico, al mismo tiempo que busca salvaguardar derechos fundamentales y asegurar la participación ciudadana en la toma de decisiones.

La Constitución Política del Perú de 1993 también se caracteriza por su énfasis en el reconocimiento de derechos fundamentales, incluyendo derechos civiles, políticos,

económicos, sociales y culturales, además, establece mecanismos para la protección y promoción de la diversidad cultural, reconociendo la pluralidad étnica y cultural del país. Este enfoque busca asegurar que todas las voces sean escuchadas y que se respete la diversidad del pueblo peruano, contribuyendo a la construcción de un estado más inclusivo, a lo largo de los años, la Constitución ha sido objeto de diversas reformas y debates, reflejando la dinámica política y social del país, pero sigue siendo un pilar fundamental en la estructura del Estado peruano y en la defensa de los derechos de sus ciudadanos.

Artículo 2.- Toda persona tiene derecho, numeral 6 A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

Es fundamental en el contexto actual, donde la recolección y tratamiento de datos personales se ha incrementado significativamente con el avance de la tecnología y la digitalización de la información. la protección de la intimidad se convierte en un imperativo ético y legal que busca resguardar aspectos esenciales de la vida privada de los individuos, derecho a la intimidad personal y familiar implica un reconocimiento de la dignidad humana y la necesidad de que los individuos tengan control sobre su propia información. La intimidad es un espacio donde las personas pueden desarrollar sus relaciones personales y familiares sin la interferencia o vigilancia de terceros, por lo tanto, la garantía de que los servicios informáticos no puedan proporcionar información que vulnere esta intimidad es crucial para la protección de la vida privada, un derecho que está intrínsecamente relacionado con la libertad y el desarrollo personal, la mención de que este derecho se aplica tanto a servicios públicos como privados resalta la importancia de que todas las entidades que manejen datos de individuos actúen con responsabilidad y respeto.

La provisión de información que afecta la intimidad puede tener consecuencias graves, desde la exposición a la vergüenza pública hasta situaciones de discriminación o persecución, en este sentido, el derecho consagrado en el artículo actúa como un mecanismo de defensa contra el uso indebido de la información personal, que puede ser utilizada para dañar la reputación, la integridad o incluso la seguridad de los individuos, esto es especialmente relevante en un mundo donde la información puede circular de manera rápida y amplia, muchas veces sin el consentimiento o el conocimiento de la persona afectada, la regulación

de este derecho es, por tanto, una herramienta fundamental para prevenir abusos y proteger a los ciudadanos de posibles daños.

Implica un desafío para las instituciones y empresas que manejan datos personales, deben implementar políticas y prácticas adecuadas para garantizar la seguridad y privacidad de la información que recopilan, procesan y almacenan, esto incluye establecer protocolos de manejo de datos que aseguren que la intimidad de las personas no sea comprometida y que se respete su derecho a controlar la información que les concierne, las entidades deben ser transparentes respecto a cómo utilizan la información y permitir a los ciudadanos acceder a sus datos, corregir inexactitudes y eliminar información que no deseen que se conserve, de este modo, se promueve un ambiente de confianza entre las instituciones y la ciudadanía.

Artículo 200.- Son garantías constitucionales:

La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos.

Artículo 200 de la Constitución Política del Perú establece la acción de hábeas data como una de las garantías constitucionales fundamentales que protege los derechos de los ciudadanos frente a acciones u omisiones que puedan amenazar o vulnerar su información personal, esta acción judicial permite que cualquier persona pueda reclamar el acceso, rectificación, actualización o supresión de datos personales que se encuentren en posesión de entidades públicas o privadas, se ha vuelto un recurso esencial y su manejo puede impactar significativamente la vida de los individuos, el hábeas data se convierte en un instrumento clave para proteger la privacidad y la dignidad personal.

La inclusión de la acción de hábeas data en la Constitución refleja el reconocimiento del derecho a la protección de datos personales como un derecho humano fundamental, este derecho no solo implica la posibilidad de acceder a la información que sobre uno se maneja, sino también la capacidad de controlar cómo se utiliza esa información, la acción de hábeas data se presenta como una herramienta necesaria para garantizar que los ciudadanos tengan voz y poder sobre sus propios datos, lo que es especialmente relevante en un mundo cada vez más digitalizado, donde la recolección y tratamiento de información personal es común.

este derecho es esencial para prevenir abusos y garantizar que las entidades que manejan datos personales lo hagan de manera responsable y respetuosa.

La acción de hábeas data también implica un aspecto de transparencia y rendición de cuentas por parte de las instituciones que manejan información personal, al permitir que los ciudadanos cuestionen y soliciten la revisión de sus datos, se fomenta una cultura de responsabilidad en el manejo de la información, esto es fundamental para fortalecer la confianza pública en las instituciones, ya que los ciudadanos deben sentir que su información está en manos seguras y que tienen el derecho de cuestionar cualquier uso indebido o incorrecto de sus datos, asimismo, al promover la protección de datos, se contribuye a la construcción de una sociedad más equitativa, en la que se respeten los derechos individuales y se garantice la dignidad de todas las personas.

### **2.2.11 Código Procesal civil de Perú**

En 2004, surge como una respuesta a la necesidad de consolidar y regular los mecanismos de defensa de los derechos fundamentales en el marco de la Constitución, durante la década de 1990, el Perú atravesó un período de crisis institucional, donde los derechos de los ciudadanos fueron vulnerados en diversos momentos, lo que generó la necesidad de fortalecer las garantías constitucionales, a raíz de estos desafíos, se vio la urgencia de contar con un marco normativo que regulase de manera clara y efectiva los procesos constitucionales destinados a la protección de los derechos fundamentales.

Antes de la promulgación del Código, la regulación de los procesos constitucionales en el Perú no estaba unificada y se encontraba dispersa en diversas normas, lo que generaba dificultades en su aplicación práctica, este código consolidó y sistematizó en un solo cuerpo normativo las diferentes garantías constitucionales, tales como el hábeas corpus, el hábeas data, la acción de amparo, y la acción popular, estas herramientas fueron diseñadas para permitir una defensa efectiva frente a las violaciones de derechos fundamentales, ya sea por parte de autoridades o particulares, el código también estableció reglas claras sobre la competencia, los plazos, y los procedimientos a seguir en este tipo de acciones, garantizando una mayor seguridad jurídica para los ciudadanos.

Un aspecto relevante de este código es su enfoque en la efectividad y celeridad de los procesos constitucionales, buscando que las demandas relacionadas con la violación de derechos fundamentales sean resueltas de manera rápida y eficiente, esto responde a la naturaleza urgente de muchos de estos casos, donde la demora en la resolución puede agravar el daño a los derechos de los ciudadanos, el Código Procesal Constitucional del Perú ha sido fundamental para asegurar que los mecanismos de defensa de los derechos sean accesibles, claros y eficaces, consolidando así el Estado de Derecho y fortaleciendo la democracia en el país.

Artículo 61.- Derechos protegidos El hábeas data procede en defensa de los derechos constitucionales reconocidos por los incisos 5) y 6) del artículo 2 de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para: 1) Acceder a información que obre en poder de cualquier entidad pública, ya se trate de la que generen, produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material.

Establece los derechos protegidos por la acción de hábeas data, un mecanismo judicial que salvaguarda los derechos constitucionales consagrados en los incisos 5) y 6) del Artículo 2 de la Constitución peruana, relacionados con el acceso a la información pública y la protección de la intimidad personal, el hábeas data es un recurso legal que permite a cualquier persona acceder a información en poder de entidades públicas, garantizando así la transparencia y el control ciudadano sobre la administración pública.

Uno de los aspectos más relevantes de este artículo es que establece que el derecho a la información no se limita a documentos o datos en formato tradicional, sino que abarca toda información en poder del Estado, sin importar el formato o el tipo de soporte material en que se encuentre, esto incluye expedientes en trámite o concluidos, dictámenes, informes técnicos, datos estadísticos, entre otros, lo que permite a los ciudadanos obtener información que puede ser crucial para ejercer sus derechos o vigilar la actuación de las autoridades públicas. En un contexto de creciente digitalización y almacenamiento de información en diferentes formatos (electrónico, visual, sonoro, entre otros), esta disposición es clave para asegurar que el derecho a la información sea amplio y eficaz.

El artículo refuerza el principio de transparencia en la gestión pública, al permitir que los ciudadanos exijan acceso a la información sin restricciones sobre la forma en que esta es almacenada o presentada, esto tiene un impacto directo en la rendición de cuentas de las instituciones públicas, ya que cualquier entidad estatal está obligada a proporcionar información que posea, lo que fomenta una cultura de responsabilidad administrativa. Además, este artículo también contribuye a la protección de la privacidad, al permitir que los ciudadanos puedan utilizar el hábeas data para proteger su información personal y asegurar que no sea usada de manera indebida por las autoridades o terceros, este derecho no solo tiene relevancia en términos de transparencia, sino que también es un instrumento esencial para garantizar el control social sobre el Estado, promoviendo una participación activa y bien informada de los ciudadanos en los asuntos públicos. El hecho de que la norma permita acceder a información en cualquier formato o soporte material es crucial, dado que muchas veces los documentos gubernamentales pueden estar en formatos digitales o en otros medios que, de no estar contemplados, podrían limitar el acceso a la información, así, el hábeas data se convierte en un mecanismo amplio y flexible para proteger los derechos fundamentales, tanto en términos de acceso a información pública como de salvaguarda de la intimidad personal.

Numeral 2.-Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales.

El Numeral 2 del artículo mencionado otorga a las personas el derecho fundamental a conocer, actualizar, incluir, suprimir o rectificar la información personal que esté almacenada en archivos, bancos de datos o registros de entidades públicas o privadas. Este derecho es una manifestación directa del principio de autodeterminación informativa, que reconoce el control personal sobre los datos que nos pertenecen, este control es esencial en un contexto donde la información personal se ha convertido en un recurso valioso y, al mismo tiempo, vulnerable, especialmente con la proliferación de tecnologías que facilitan la recopilación y el tratamiento masivo de datos.



Uno de los aspectos clave del texto es que se menciona que la información puede estar almacenada de manera manual, mecánica o informática, lo que implica que el derecho de las personas a gestionar sus datos no está limitado a ningún formato en particular, esto es crucial en una era de digitalización, donde las bases de datos electrónicas son omnipresentes, pero también pueden existir archivos físicos o mecánicos con información sensible, el derecho de actualizar, suprimir o rectificar los datos asegura que las personas puedan corregir información inexacta o desactualizada que puede afectar su vida personal, profesional o incluso su reputación.

#### **2.2.12 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional de Perú**

En Perú, no existe una ley orgánica específica sobre garantías jurisdiccionales y control constitucional en el tema de hábeas data porque este derecho está regulado dentro del marco general de protección constitucional y no se ha considerado necesario crear una ley única para tales garantías, el hábeas data está reconocido en la Constitución Política del Perú, dentro de esta estructura descentralizada del control constitucional en Perú permite que cualquier juez pueda resolver acciones de hábeas data, sin la necesidad de una ley orgánica concentrada.

#### **2.2.13 Ley orgánica de protección de datos**

No existe una Ley Orgánica de Protección de Datos específicamente enfocada en el hábeas data es porque este derecho está contemplado y regulado en diversas leyes que abordan la protección de datos personales de manera más amplia y descentralizada, estas leyes establecen los derechos y procedimientos para que las personas puedan acceder, rectificar, actualizar o eliminar la información personal que se encuentre en bases de datos, sin necesidad de una ley orgánica específica que se concentre únicamente en el hábeas data, el enfoque fragmentado responde a la necesidad de abarcar no solo la protección de datos a través del hábeas data, sino también otros aspectos más amplios relacionados con el manejo de la información personal en el ámbito digital, comercial y administrativo.

#### **2.2.14 Ley de comercio electrónico, firma y mensajes de datos**

En Perú, no existe una ley específica que unifique el comercio electrónico, las firmas electrónicas y los mensajes de datos en el contexto del hábeas data porque estos temas se encuentran regulados de manera dispersa en diversas normativas, el hábeas data, como garantía constitucional para proteger los datos personales esto regula su uso para la protección y control de la información personal.

#### **2.3 Marco Conceptual**

**Derecho genérico:** es aquel ordenamiento jurídico que nace para el efecto de regular la conducta entre los individuos.

**Previsibilidad:** cualidad de aquello cuyo acontecimiento puede ser conocido o conjeturado anticipadamente.

**Estigmatización:** conjunto de actitudes y creencias desfavorables que desacreditan o rechazan a una persona o grupo.

**Perpetuar:** hacer perpetuo o perdurable

**Supresión:** derecho a eliminar ocultar y cancelar aquellas informaciones o hechos pasados de la vida de las personas.

**Inexactitud:** falta de exactitud imprecisión, indeterminación, vaguedad, falsedad

**Tácito:** que no entiende percibe o oye o dice formalmente

**Incertidumbre:** falta de información, grado de desconocimiento

## **CAPÍTULO III**

### **MARCO METODOLÓGICO**

#### **3.1. Diseño y tipo de investigación**

##### **Diseño de investigación**

La presente investigación denominada “Estudio comparado a las reglas de habeas data de las legislaciones de Ecuador, Argentina y Perú (2024)” fue realizada bajo el enfoque cualitativo, teóricamente permite interpretar y comprender la realidad, cuya metodología se estructura a partir de la formulación del problema vinculado a las reglas del Hábeas Data, por medio de la recolección de datos estudiando distintas legislaciones y realidades en los países de Ecuador, Argentina y Perú.

El problema se analizó en cada uno de los aspectos interesantes de la situación actual de las Constituciones y garantía constitucional Hábeas data en Ecuador, Argentina y Perú, a través de un estudio comparativo, se interpretaron las legislaciones de las naciones objeto de estudio, además, para identificar similitudes y diferencias en la aplicación de Hábeas data se utilizaron diversos métodos y técnicas de investigación.

##### **Tipo de investigación**

El tipo de investigación en este estudio fue exploratorio, se realiza especialmente cuando el tema elegido ha sido poco explorado, reconocido y cuando aún, sobre él, es difícil formular hipótesis precisas o de cierta generalidad, se realizó una recolección de información sobre el tema con el objeto de estudio generando una hipótesis acerca de las reglas de la acción constitucional respectiva al derecho a la información y acceso a los datos personales explicando las características fundamentales del problema legal que versa sobre la eficacia de la accesibilidad de los datos personales del propio titular explorando las diferencias y similitudes del recurso en Ecuador, Argentina y Perú.

### 3. 2 Recolección de la información

En este estudio la recolección de datos contempla la agrupación de elementos relativos al fenómeno de estudio a través de técnicas de investigación para obtener información, la población comprende la agrupación de objetos accesibles para la elección de la muestra lo que permite conocer las características del fenómeno de investigación, siendo posible definir el número total de individuos en el estudio comparado que serán parte del proceso de investigación para concretar el problema de la investigación. La información comprenderá las siguientes legislaciones:

Tabla #4 Población

PAISES	POBLACIÓN	TOTAL
<b>ECUADOR</b>	Constitución de la República del Ecuador	1
	Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional	1
	Ley Orgánico de datos personales	1
	Ley de Comercio electrónico, firmas y mensajes de datos	1
<b>ARGENTINA</b>	Constitución Nacional de Argentina	1
	Ley de acceso a la información. Ley 27,275	1
<b>PERÙ</b>	Constitución Política de Perú	1
	Código procesal civil de Perú	1
<b>TOTAL</b>		8

Elaborado por: Katherine Cornejo

La muestra es una parte perteneciente a la población total de la investigación, por lo tanto, en el presente estudio de comparación jurídica, la población abarca la recopilación de información de las normas legales de Ecuador, Argentina y Perú, siendo impracticable por su naturaleza aplicar un muestreo a la población.

## **Métodos, Técnicas e Instrumentos**

### **Método**

En el trabajo de investigación, la recolección de la información se realizó mediante estrategias para analizar y comprender la información de manera objetiva, manifiesta que los métodos orientan los pasos a seguir en la investigación para dar a conocer el fenómeno de estudio, aquellos métodos que nos permitió desarrollar la investigación sobre el estudio comparado de las reglas de Hábeas Data para lograr los objetivos propuestos, a continuación, son:

El método analítico da cuenta del objeto de estudio del grupo de investigación que en este trabajo se ocupa, con una rigurosa investigación documental, del método mismo que orienta su quehacer, este método permitió el análisis exhaustivo de las normativas legales de Ecuador, Argentina y Perú, en ese sentido, nos ayudó a obtener los datos requeridos y facilitó la comprensión del fenómeno de estudio por medio de la descomposición de elementos obteniendo una conclusión general reconstruida por la examinación de la doctrina sobre el Hábeas Data.

El método comparación jurídica dentro del objeto de estudio es el procedimiento de comparación sistemática que se emplea para formular generalizaciones a partir de bases teóricas basadas en la experiencia para llegar a la verificación de hipótesis, el método comparativo nos brindó soporte en el análisis para contrastar e identificar similitudes en la aplicación de las reglas de habeas data de las legislaciones de Ecuador, Argentina y Perú con la finalidad de comprender e interpretar las diferentes teorías acerca de la protección de datos personales.

El método exegético se considera como una ciencia que su propia naturaleza asume una arista interpretativa que se vincula con la interpretación y aplicación de las normas e instituciones jurídicas, tanto sustantivas como adjetivas, así como el actuar de los organismos y operadores turísticos, en ese sentido, es fundamental en la investigación para interpretar y analizar las legislaciones de los países objeto de estudio de manera rigurosa y profunda, permitiendo una comprensión más completa y enriquecedora sobre la eficacia de

la protección de las normas que versan el derecho a la información y protección de datos personales.

### **Técnicas e instrumentos**

Las técnicas empleadas en el proyecto de investigación es la técnica de fichaje, misma que se centra en organizar, registrar, recopilar información relevante de fuentes confidenciales, de esta manera permitió conocer a profundidad las normativas correspondientes a Estudio comparado a las reglas de habeas data de las legislaciones de Ecuador, Argentina y Perú (2024)<sup>2</sup> en los países comparados y por último se utilizó la técnica de resumen que se caracteriza por condensar información específica y concisa ya sea de un texto o fuentes verídicas. Esta técnica fue de gran utilidad porque permitió desarrollar una investigación precisa del tema, obteniendo una base argumentativa del uso y tenencia de armas blancas en los países comparados.

Para analizar cada uno de los elementos del fenómeno de estudio sobre la aplicación del hábeas data, el cual consiste en conseguir información a través de la revisión de documentos relevantes, como doctrinas, legislaciones vigentes, entre otros, estos documentos fueron seleccionados y evaluados para la interpretar y analizar las reglas relacionadas con la acción del hábeas data y la eficacia de su aplicación.

Para el contraste del objeto de estudio por sus similitudes y diferencias referente al Hábeas Data se empleó la comparación jurídica, el cual se realizó un análisis comparativo de las normas legales aplicadas en Ecuador, Argentina y Perú, así mismo, se utilizó la técnica del resumen para interpretar las ideas principales de las bases teóricas de documentos.

### **3. 3. Tratamiento de la información**

Tras obtener toda la información requerida mediante el procedimiento metodológico explicado previamente y la aplicación de diversas técnicas de investigación con el propósito de respaldar las afirmaciones a través de fichas bibliográficas y citas durante el desarrollo de este trabajo; es crucial resaltar la diversidad de documentación doctrinal utilizada, que abarca tesis, revista y libros científicos, así como la consulta de diccionarios. Cabe recalcar que la

recopilación de información se llevó a cabo tanto en la biblioteca virtual como en la física de la Universidad Estatal Península de Santa Elena, así como en las páginas web de confianza, estableciendo a estos recursos el papel esencial en el contexto referencial de la investigación.

En la presente investigación, se exploraron conceptos que engloban la revisión histórica, el funcionamiento, las medidas y otros elementos fundamentales relacionados con las variables de estudio, esta variable se centra en el estudio de las reglas del habeas data, donde se empleó como enfoque principal el método de derecho comparado, analizando las legislaciones pertinentes Ecuador, Argentina y Perú.

En este contexto, se abordaron detalladamente los antecedentes históricos que han influido en la conceptualización y evolución de la garantía del habeas data, así como los mecanismo y medidas adoptadas para la protección de datos, utilizando el derecho comparado como herramienta para identificar similitudes y diferencias y mejores prácticas en la aplicación de esta garantía constitucional.

Así mismo, se profundizó en el análisis del tratamiento de los datos personales como un derecho crucial en el marco de protección de datos, se revisaron las legislaciones de los países mencionados para comprender como abordan la garantía del habeas data, destacando las estrategias legales y las medidas implementadas para mitigar los efectos de vulneración a esta garantía constitucional.

### 3.4. Operacionalización de las variables

Tabla #5 Operacionalización de las variables

TITULO	VARIABLES	CONCEPTO	DIMENSIONES	INDICADORES	ITEMS	INSTRUMENTOS
<b>Estudio comparado a las reglas de habeas data de las legislaciones de Ecuador, Argentina y Perú 2024</b>	Univariable	Es una garantía constitucional que permite a los ciudadanos acceder, rectificar, actualizar y eliminar información personal en bases de datos públicas y privadas, para la operacionalización se realizó en un estudio comparado entre Ecuador, Argentina y Perú, se analizarán las diferencias en los marcos legales, mecanismos de acceso, rectificación y protección de datos, así como la aplicación judicial y administrativa. También se evaluará la eficacia de las sanciones y el nivel de conocimiento ciudadano sobre este derecho en cada país.	Reglas de habeas data	Antecedentes y evoluciones del Habeas Data	garantía procesal de habeas data	Ficha bibliográfica  Matriz de comparación
			Marco constitucional Legislación Ecuatoriana	enfoques constitucionales del Habeas Data	acceso a la información y el derecho a la protección de datos personales	Ficha bibliográfica  Matriz de comparación
	Legislación de Argentina		Reconocimiento del derecho a la protección de la garantía del habeas data	cambios legislativos en las 3e legislaciones	Ficha bibliográfica  Matriz de comparación	
	Legislación de Perú		Reconocimiento del derecho al libre acceso al habeas data	Enfoques doctrinales	Ficha bibliográfica  Matriz de comparación	

Elaborado por: Katherine Cornejo



## CAPÍTULO IV

### RESULTADOS Y DISCUSIÓN

#### 4.1 Análisis, interpretación y discusión de los resultados

La presente matriz de comparación, permitió evidenciar las diferencias y similitudes de las legislaciones de Ecuador, Argentina y Perú respecto al estudio comparado a las reglas de habeas data de las legislaciones de los países ya mencionados, desde esta perspectiva, el método comparativo fue una herramienta de ayuda para poder evidenciar las realidades de las tres legislaciones de las reglas del habeas data, a través de la matriz se logró realizar descripciones, criterios de cada subtema mencionado despejando las diferentes ventajas y desventajas dentro de cada una de las legislaciones comparadas.

*Tabla #6 Matriz Comparativa*

PAÍS	DIFERENCIAS	SEMEJANZAS
<b>ECUADOR</b>	Protege el derecho al acceso de la información personal. Reconoce el derecho al honor, buen nombre, intimidad e imagen.	No se exige requerimiento previo alguno que deba formular el actor ante el registro que mantiene su información personal.
<b>ARGENTINA</b>	la Corte Suprema de Justicia de la Nación fijó su posición en materia de información reservada obrante en los registros, archivos, bases o bancos de datos públicos,	la LEY 25.326 cuya normativa excede el marco del instituto del habeas data, pues tiene por objeto la "protección de los datos personales". A través de sus disposiciones se establecen los principios generales relativos a la protección de los datos, garantiza a toda persona el poder de control sobre los mismos, sobre su uso y destino
<b>PERÚ</b>	Protege el derecho al acceso de la información personal.  Es requisito la negación por parte de la autoridad o administrador de la información.	Procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza derechos personales.

**Fuente: Constitución de las tres legislaciones Ecuador, Argentina, Perú y Garantías Jurisdiccionales**  
**Elaborado por: Katherine Cornejo**

Tabla #7 Matriz de Alcance y Protección del Habeas Data

País	Derechos Protegidos	Tipos de Datos	Sujetos Obligados	Excepciones
<b>Ecuador</b>	Los derechos protegidos son; el acceso a la información personal, ratificación de datos actualización de la información, eliminación de datos, protección contra usos indebidos, reserva de información sensible, control de datos en bases y transparencia en el manejo de datos	Datos personales Datos anonimizados Datos seudonimizados Datos públicos Datos privados Datos de menores de edad Datos financieros Datos laborales	Entidades públicas Entidades privadas Personas naturales y jurídicas Operadores de las plataformas tecnológicas Medios de comunicación Empresas internacionales con operaciones en Ecuador	Estas excepciones están orientadas a proteger otros derechos fundamentales, el interés público o la seguridad del Estado: <ul style="list-style-type: none"> <li>• Información relacionada con la seguridad nacional</li> <li>• Información confidencial de tercero</li> <li>• Informaciones protegidas por secreto profesional o legal</li> <li>• Investigaciones judiciales en cursos</li> <li>• Información de menores de edad</li> <li>• Protección del orden público moral</li> <li>• Excepciones en el ámbito laboral</li> </ul>
<b>Argentina</b>	En Argentina los derechos protegidos por la garantía del habeas data son específicamente los siguientes: acceso a la información, corrección y actualización de datos, supresión de datos, control de uso de datos personales, privacidad, prohibición de almacenamiento discriminatorio, información previa al tratamiento.	Datos personales Datos sensibles Datos no sensibles Datos anonimizados Datos públicos Datos crediticios Datos de menores de edad	Responsables de bases de datos públicos, organismos gubernamentales Responsables de bases de datos privadas empresas de telecomunicaciones, bancarias, clínicas, empresas de marketing. Proveedores de servicios digitales y tecnológicos redes sociales empresas de comercio electrónico, almacenamientos en las nubes	La exepciones en argentina se limitan especialmente cuando entran con conflicto con otros derechos como, por ejemplo: <ul style="list-style-type: none"> <li>• Información relacionada con la defensa y seguridad nacional, ejemplo la Agencia Federal de Inteligencia.</li> <li>• Investigación judicial o policial en curso (antecedentes penales en investigaciones aún no resuelta)</li> </ul>

			Agencias de formes crediticios y comerciales, que la información sea precisa y actualizada, permitir a titulares a ratificar errores o eliminación de información obsoleta.	<ul style="list-style-type: none"> <li>• Datos de terceros que puedan ser vulnerados</li> <li>• Fuentes públicas accesible a la comunidad.</li> </ul>
<b>Perú</b>	Regulado en el Código Procesal Constitucional los derechos protegidos en Perú refieren, derecho de acceso a la información personal, derecho de ratificación, derecho de cancelación, derecho de oposición, derecho de la autodeterminación informativa, derecho a la privacidad y confidencialidad, derecho al consentimiento informado derecho a o la transparencia en el tratamiento de datos.	Perú clasifica en función de su naturaleza y nivel de sensibilidad. Datos personales datos sensibles Datos públicos datos anonimizados Datos no sensibles Datos financieros Datos biométricos Datos de menores de edad	Po su naturaleza jurídica públicas o privadas: 1.- responsables del tratamiento aseguradoras u organismos 2.- encargados del tratamiento de datos personales 3.-entidades públicas 4.- Autoridad Nacional de Protección de Datos Personales ANPDP. 5.- personas jurídicas que manejan datos sensibles	<ul style="list-style-type: none"> <li>• Las exepciones reconocidos en la Constitución Política de Perú buscan equilibrar la protección de datos con otros derechos e intereses legítimos.</li> <li>• Información gestionada por las Fuerzas Armadas o la Policía Nacional de Perú</li> <li>• Datos obtenidos en investigaciones sobre terrorismo.</li> <li>• Información recopilada por el ministerio público en una investigación penal.</li> <li>• Registro de interceptaciones telefónicas autorizadas judicialmente.</li> <li>• No se puede acceder a datos protegidos por el secreto profesional</li> <li>• El habeas data no es aplicable cuando el ejercicio de esta garantía pueda afectar la privacidad o derechos de otra persona.</li> </ul>

Elaborado por Katherine Cornejo

Tabla # 8 Matriz de Fundamentos Constitucionales y Legales

País	Base Constitucional	Leyes Específicas	Año de Implementación
<b>Ecuador</b>	<p>Constitución de la Republica del Ecuador</p> <p><b>Artículo 66</b> Se reconoce y garantiza el derecho a la protección de datos personales. Este derecho incluye el acceso, la rectificación y la cancelación de la información personal contenida en bases de datos públicas o privadas</p> <p><b>Artículo 22</b> Las personas tienen derecho a acceder a la información y a los datos personales contenidos en bases de datos públicas o privadas. La ley regulará el acceso a la información pública y la protección de los datos personales.</p> <p><b>Artículo 23</b> La Constitución garantiza el derecho a la privacidad y a la protección de la información personal. La ley regulará la recolección, el almacenamiento y la difusión de la información personal.</p> <p><b>Artículo 94</b> El habeas data es un recurso que se ejerce ante un juez para garantizar el derecho a la protección de datos personales. La ley regulará el procedimiento para la presentación y resolución del habeas data.</p>	<p>Ley Orgánica de Protección de Datos Personales (LOPD), regula la protección de datos personales en Ecuador y establece los principios y normas para el tratamiento de datos personales</p> <p>Ley de Acceso a la Información Pública (LAIP), Esta ley regula el derecho de acceso a la información pública en Ecuador y establece los procedimientos para acceder a la información pública</p> <p>Código de la Niñez y Adolescencia (CNA), específicamente regula la protección de los derechos de los niños y adolescentes en Ecuador, incluyendo la protección de sus datos persona</p> <p>Ley de Comercio Electrónico (LCE), establece el comercio electrónico en Ecuador y propone normas para la protección de los datos personales en el ámbito del comercio electrónico.</p> <p>Reglamento General de Protección de Datos Personales (RGPD), ordena la protección de datos personales en Ecuador y establece normas para el tratamiento de datos personales.</p>	<p>La garantía del habeas data en Ecuador se implementó por primera vez en el año 1996, en la codificación constitucional publicada en el Registro Oficial No. 969 de 18 de diciembre de ese año</p> <p>la Ley Orgánica de Protección de Datos Personales, que fue promulgada en 2011, esta ley regula la protección de datos personales y establece los principios y normas para el tratamiento de datos personales.</p> <p>La Ley Orgánica de Transparencia y Acceso a la Información Pública en Ecuador se reguló en el año 2004. Posteriormente, esta ley sufrió una reforma en el año 2009, específicamente el 28 de septiembre de ese año, mediante la Disposición General Primera de la Ley s/n, R.O. 35-S.}</p> <p>La Ley de Comercio Electrónico en Ecuador se implementó en el año 2002. Desde ese año regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.</p> <p>El Reglamento General de Protección de Datos Personales en Ecuador se creó en el año 2023, mediante el Decreto Ejecutivo No. 904, publicado el 10 de noviembre de ese año.</p>

<p><b>Argentina</b></p>	<p>Constitución de la República de Argentina</p> <p>Artículo 43 Toda persona puede interponer acción expedita y rápida de hábeas data para tomar conocimiento de los datos personales que sean objeto de tratamiento por parte de organismos públicos o privados y, en su caso, para solicitar su rectificación, actualización o supresión.</p> <p>Artículo 75, Inciso 22 Corresponde al Congreso: (...) 22. Dictar los códigos Civil, Comercial, Penal, de Procedimientos y de la navegación, en cuyo ejercicio serán de aplicación las siguientes bases: (...) La protección de los derechos de los usuarios y consumidores y la defensa de la competencia contra toda forma de distorsión de los mercados, en el marco de una economía social de mercado. La legislación establecerá las normas de protección de datos personales y su régimen de tratamiento.</p>	<p>Leyes Nacionales</p> <p>Ley 25.326 de Protección de Datos Personales (2000), regula la protección de datos personales en Argentina y establece los principios y normas para el tratamiento de datos personales.</p> <p>Ley 26.951 de Modificación de la Ley 25.326 (2014) modifica la Ley 25.326 y establece nuevas normas para la protección de datos personales, incluyendo la creación de Reglamentos</p> <p>Decreto 1558/2001: Reglamento de la Ley 25.326 de Protección de Datos Personales.</p> <p>Resolución 10/2009: Reglamento de la Agencia de Acceso a la Información Pública.</p>	<p>La garantía del hábeas data se estableció en la Constitución de Argentina en 1994, específicamente a través de la reforma constitucional de ese año, que incluyó el artículo 43.</p> <p>La ley nacional específicamente del habeas data en Argentina es la Ley 25.326 de Protección de Datos Personales, sancionada el 4 de octubre de 2000 y promulgada parcialmente el 30 de octubre de 2000.</p> <p>El reglamento sobre el hábeas data en Argentina se creó en el año 2001, mediante el Decreto 1558/2001, que reglamenta la Ley 25.326 de Protección de Datos Personales</p>
<p><b>Perú</b></p>	<p>Constitución Política del Perú</p> <p>Artículo 2, Inciso 5.-Toda persona tiene derecho a la protección de su intimidad personal y familiar. Los documentos privados, las comunicaciones y la correspondencia son inviolables.</p> <p>Artículo 2, Inciso 6.- Los ciudadanos tienen derecho a acceder a la información y a los datos que sobre ellos se contengan en registros o bancos de datos públicos o privados.</p> <p>Código Civil Artículo 2.- Reconoce el derecho a la intimidad y la protección de la vida privada. Artículo 5.- Establece el derecho a la autodeterminación informativa, que incluye el</p>	<p>Leyes Nacionales</p> <p>Ley de Protección de Datos Personales Ley N° 29733: Esta ley regula la protección de datos personales en Perú y establece los principios y normas para el tratamiento de datos personales.</p> <p>Ley de Transparencia y Acceso a la Información Pública Ley N°27806.-regula el derecho de acceso a la información pública y establece los mecanismos para ejercer este derecho.</p> <p>Reglamento de la Ley de Protección de Datos Personales</p>	<p>la Constitución de 1993 reconoce el derecho al habeas data en su artículo 200. Sin embargo, la ley específica que regula la protección de datos personales es la Ley de Protección de Datos Personales, que fue promulgada en 2011 y aplicada en 2015</p> <p>En Perú, los reglamentos del habeas data fueron regulados en el año 2013, específicamente a través del Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales Ley N° 29733.</p>

	<p>derecho a acceder, rectificar y cancelar datos personales.</p> <p>Código Procesal Civil  Artículo 3.- Reconoce el derecho a la intimidad y la protección de la vida privada.  Artículo 734.- Establece el procedimiento para la protección de datos personales y el derecho al hábeas data.</p> <p>Código de Protección y Defensa del Consumidor  Artículo 3.- Reconoce el derecho a la protección de los datos personales de los consumidores.  Artículo 39.- Establece la obligación de los proveedores de servicios de respetar la privacidad y la confidencialidad de los datos personales de los consumidores.</p>	<p>Decreto Supremo N° 003-2013-JUS, Específicamente este reglamento establece las normas y procedimientos para la implementación de la Ley de Protección de Datos Personales.</p> <p>Reglamento de la Ley de Transparencia y Acceso a la Información Pública</p> <p>Decreto Supremo N° 072-2003-PCM, generalmente este reglamento establece las normas y procedimientos para la implementación de la Ley de Transparencia y Acceso a la Información Pública.</p>	
--	--	--	--

**Elaborado por: Katherine Cornejo**

Tabla # 9 Matriz de Aspectos Procesales

País	Autoridad Competente	Plazo de Resolución	Requisitos de Admisibilidad	Recursos Disponibles
<b>Ecuador</b>	<p><b>Autoridades judiciales</b></p> <p>1.- Jueces de garantías penales, quienes son encargados de conocer y resolver las acciones del habeas data con la protección de datos personales en el ámbito penal.</p> <p>2.- Jueces civiles, competentes para resolver la protección de datos en el ámbito civil.</p> <p><b>Autoridades administrativas</b></p> <p>1.- Super Intendencias de la Información y Comunicación (SUPERCOM) encargada de proteger los derechos de las personas en relación con la información y la comunicación incluyendo datos personales.</p> <p>2.- Agencias de Regulación y Control de Comunicaciones (ARCOTEL) controla las comunicaciones en Ecuador incluyendo la protección de datos en las telecomunicaciones</p> <p>Otras autoridades</p>	<p>La Corte Constitucional ha interpretado que un plazo razonable es aquel que permite satisfacer el derecho del solicitante de manera oportuna y eficaz. Esto dependerá de la cantidad de información requerida, el tipo del pedido y la conducta de la persona o institución que posea la información.</p> <p>En general, el procedimiento de la garantía del habeas data debe ser sencillo, rápido y eficaz, y debe ser oral en todas sus fases e instancias. Sin embargo, es importante mencionar que los plazos específicos pueden variar dependiendo del caso concreto y autoridad competente que lo resuelva.</p> <p>Estos plazos se encuentran en la resolución mediante la sentencia N°182-15-sep-cc Corte Constitucional.</p>	<p>Requisitos generales</p> <p>Legitimación activa: puede ser presentado por cualquier persona que considere que sus derechos a la protección de datos están siendo vulnerados.</p> <p>Interés legítimo. – el solicitante debe demostrar que tiene un interés legítimo en la protección de sus datos personales</p> <p>Requisitos específicos</p> <p>Identificación del solicitante</p> <p>Descripción de los hechos</p> <p>Identificación de la persona o institución demandada</p> <p>Solicitud concreta</p> <p>Documentación requerida</p> <p>Copia de cédula de ciudadanía</p> <p>Documentación que acredite</p>	<ul style="list-style-type: none"> <li>▪ Recurso de habeas data: Acción de Acceso de Información</li> <li>▪ Recurso de Amparo Superintendencia de Información y Comunicación</li> <li>▪ Defensoría del pueblo</li> </ul>
	<p>1.-Defensoría del pueblo, promueve los Derechos Humanos a la Protección de Datos Personales</p> <p>2.-Consejo Nacional para la igualdad de género, encargada de velar por los derechos de las mujeres y otros grupos vulnerables relacionados a la protección de datos</p>		<p>Otros documentos que resulten relevante para su caso</p>	

<p><b>Argentina</b></p>	<p>Las autoridades competentes en Argentina para resolver el habeas data son:</p> <p><b>Autoridades judiciales</b></p> <p>1.- Jueces de primera instancia de lo civil</p> <p>2.- Jueces de primera instancia de lo penal</p> <p>3.-Cámara Nacional de Apelaciones en lo Civil y Comercial</p> <p>4.- Cámara Nacional de Apelaciones en lo Penal</p> <p><b>Autoridades administrativas</b></p> <p>1.- Agencias de Acceso de la Información Pública</p> <p>2.- Dirección Nacional de Protección de Datos Personales</p> <p>3.-Defensor del Pueblo de la Nación</p>	<p>En Argentina los plazos de resolución del habeas data varían según la autoridad competente y complejidad del caso:</p> <p>Jueces de primeras instancias de 10 a 30 días hábiles para resolver habeas data</p> <p>Cámara Nacional de Apelaciones 30 a 60 días hábiles para resolver el recurso de apelación</p> <p>Plazos especiales</p> <p>Habeas data urgente 24 a 48 horas para resolver en casos de urgencias o peligro eminente</p> <p>Habeas data con medida cautelar 5 a 10 días hábiles</p> <p>Cabe mencionar que estos plazos pueden variar, además de que es posible que se requieran pruebas adicionales o se solicite informes de terceros lo que puede prolongar el plazo de resolución.</p>	<p><b>Requisitos generales</b></p> <p>Legitimación activa; presentado por cualquier persona.</p> <p>Legitimación pasiva; se dirige contra la persona o institución que posea o controle los datos personales</p> <p>Interés legítimo; el solicitante debe demostrar su interés a la protección de sus datos</p> <p><b>Requisitos específicos</b></p> <p>Identificación del solicitante</p> <p>Descripción de los hechos identificación de la persona o institución demandada</p> <p>Solicitud concreta</p> <p>Documentación requerida</p> <p>Copia de cédula de identidad</p>	<ul style="list-style-type: none"> <li>▪ <b>Recursos judiciales</b> Recurso de habeas data, permite garantizar sus derechos a la protección de datos Recurso de amparo que permite solicitar protección de sus derechos fundamentales Recurso de queja, permite solicitar la revisión de una decisión judicial</li> <li>▪ <b>Recursos administrativos</b> Agencia de Acceso de Información Pública Dirección Nacional de Protección de Datos Personales Defensor del Pueblo de la Nación</li> <li>▪ <b>Recurso de segundo grado</b> Cámara Nacional de lo Civil y Comercial Cámaras Nacionales de Apelación Corte Suprema de Justicia de la Nación, encargados de resolver recursos de casación interpuesta contra las sentencias dictadas</li> </ul>
	<p>4.-Comisión Nacional de Protección de Datos Personales</p>		<p>Documento que acredite la vulneración del derecho</p> <p>Otros documentos que se considere relevante para su caso</p>	



<p><b>Perú</b></p>	<p>En Perú entre las autoridades competentes están:</p> <p><b>Autoridades judiciales</b></p> <p>1.- Jueces de Paz Letrados. - especializados en resolver habeas data en lo civil y penal</p> <p>2.- Corte Superiores de Justicia. - expertos en resolver apelaciones interpuesta contra sentencias dictada</p> <p>3.- Tribunal Constitucional. - es la autoridad máxima en materia de derecho constitucional y puede resolver ele habeas data</p> <p><b>Autoridades administrativas</b></p> <p>1.- Autoridad Nacional De Protección De Datos Personales. - garantiza el derecho del habeas data</p> <p>2.- Defensoría Del Pueblo. - promueve los derechos humanos en Perú incluyendo los derechos del habeas data</p> <p>Otras autoridades</p> <p>1.- Instituto Nacional De Estadísticas e Informática</p>	<p>Jueces de Primera Instancia: 10 a 30 días hábiles para resolver el hábeas data.</p> <p>Cámara Nacional de Apelaciones: 30 a 60 días hábiles para resolver el recurso de apelación.</p> <p>Corte Suprema de Justicia de la Nación: 60 a 120 días hábiles para resolver el recurso de casación.</p> <p>Plazos Administrativos</p> <p>Agencia de Acceso a la Información Pública (AAIP): 10 a 30 días hábiles para resolver el hábeas data.</p> <p>Dirección Nacional de Protección de Datos Personales: 30 a 60 días hábiles para resolver el hábeas data.</p> <p>Plazos Especiales</p> <p>Hábeas data urgente: 24 a 48 horas para resolver el hábeas data en casos de urgencia o peligro inminente.</p> <p>Hábeas data con medida cautelar: 5 a 10 días hábiles para resolver la medida cautelar solicitada.</p> <p>Es importante mencionar que estos plazos pueden variar según la complejidad del caso y la carga de trabajo de la autoridad competente. Además, es posible que se requieran pruebas adicionales o se soliciten informes de terceros, lo que puede prolongar el plazo de resolución.</p>	<p><b>Requisitos Generales</b></p> <p>Legitimidad activa: El hábeas data puede ser presentado por cualquier persona que considere que sus datos personales han sido vulnerados.</p> <p>Legitimidad pasiva: El hábeas data se dirige contra la persona o institución que posea o controle los datos personales del solicitante.</p> <p>Interés legítimo: El solicitante debe demostrar que tiene un interés legítimo en la protección de sus datos personales.</p> <p><b>Requisitos Específicos</b></p> <p>Identificación del solicitante: El solicitante debe identificarse plenamente y proporcionar su dirección y otros datos de contacto.</p> <p>Descripción de los hechos: El solicitante debe describir los hechos que considera que vulneran sus derechos relacionados con la protección de datos personales.</p> <p>3. Identificación de la persona o institución demandada: El solicitante</p>	<p><b>Recursos Judiciales</b></p> <ul style="list-style-type: none"> <li>▪ Recurso de Hábeas Data. - Es un recurso judicial que permite a las personas solicitar la protección de sus datos personales y garantizar su derecho a la privacidad.</li> <li>▪ Recurso de Amparo. - Es un recurso judicial que permite a las personas solicitar la protección de sus derechos fundamentales, incluyendo el derecho al hábeas data.</li> <li>▪ Recurso de Queja. -Es un recurso judicial que permite a las personas solicitar la revisión de una decisión judicial que considere que vulnera sus derechos.</li> </ul> <p><b>Recursos Administrativos</b></p> <ul style="list-style-type: none"> <li>▪ Autoridad Nacional de Protección de Datos Personales. - Es la autoridad administrativa encargada de proteger los datos personales y garantizar el derecho al hábeas data.</li> <li>▪ Defensoría del Pueblo. - Es la institución encargada de proteger y promover los derechos humanos en Perú, incluyendo el derecho al hábeas data.</li> </ul>
--------------------	--	--	---	--

	<p>2.- Super Intendencia De Banca Seguros Y Administración Privada De Fondos De Pensiones. - encargada de supervisar y regular entidades financieras y aseguradoras en materia de protección de datos personales.</p>		<p>debe identificar plenamente a la persona o institución que posea o controle los datos personales del solicitante. Solicitud concreta: El solicitante debe formular una solicitud concreta y específica relacionada con la protección de sus datos personales. Documentación Requerida Copia de la cédula de identidad: El solicitante debe presentar una copia de su cédula de identidad. Documentación que acredite la vulneración de derechos: El solicitante debe presentar documentación que acredite la vulneración de sus derechos relacionados con la protección de datos personales. Otros documentos: El solicitante puede presentar otros documentos que considere relevantes para su caso.</p>	<p><b>Recursos de Segundo Grado</b></p> <ul style="list-style-type: none"> <li>▪ Corte Superior de Justicia. -Es la autoridad judicial encargada de resolver los recursos de apelación interpuestos contra las sentencias dictadas por los jueces de primera instancia.</li> <li>▪ Corte Suprema de Justicia de la República. -Es la autoridad judicial máxima en Perú, encargada de resolver los recursos de casación interpuestos contra las sentencias dictadas por las cortes superiores.</li> </ul> <p><b>Otros Recursos</b></p> <ul style="list-style-type: none"> <li>▪ Instituto Nacional de Estadística e Informática (INEI). - Es la autoridad encargada de proteger y garantizar el acceso a la información estadística y de datos personales.</li> <li>▪ Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS). - Es la autoridad encargada de supervisar y regular a las entidades financieras y aseguradoras en materia de protección de datos personales.</li> </ul>
--	---	--	--	--

Elaborado por: Katherine Cornejo

Tabla #10 matriz normativa principal

ASPECTO	ECUADOR	ARGENTINA	PERÚ
<b>Normativa principal</b>	<p>La normativa principal en Ecuador sobre el habeas data se encuentra en la Constitución del Ecuador, específicamente en el artículo 94, que establece el derecho a la protección de los datos personales. Además, la Ley Orgánica de Protección de Datos Personales es la normativa principal que regula la protección de datos personales en Ecuador. Esta ley establece los principios y normas para el tratamiento de datos personales, así como los derechos de los titulares de los datos y las obligaciones de los responsables del tratamiento de datos.</p>	<p>La normativa principal que regula el habeas data en Argentina esta establecida en la Constitución Nacional en su Artículo 43. Este artículo establece el derecho a la protección de los datos personales y la obligación del Estado de garantizar la seguridad y la privacidad de estos. Seguidamente de la Ley de Protección de Datos Personales Ley N° 25.326 que regula la protección de datos personales y establece los principios y normas para el tratamiento de datos personales.</p>	<p>La normativa principal en Perú sobre el hábeas data es:</p> <p>La Constitución Política del Perú Artículo 2, Inciso 5 que reconoce el derecho a la protección de la intimidad personal y familiar. Seguido del Inciso 6 que Establece el derecho a acceder a la información y a los datos que sobre uno se contengan en registros o bancos de datos públicos o privados.</p> <p>Por otra parte, la Ley de Protección de Datos Personales Ley N° 29733 que Regula la protección de datos personales y establece los principios y normas para el tratamiento de datos personales.</p>

**ANALISIS:** las legislaciones de Ecuador Argentina y Perú establecen normativas principales que regulan la protección de datos personales y la garantía del habeas data. Aunque existen similitudes en los principios y normas establecidos, cada país tiene su propias particularidades y sanciones en materias de datos personales. EJEMPLO: en Ecuador proponen sanciones penales y administrativas para los responsables del tratamiento de datos que incumplan la ley, en cambio en Argentina y Perú coinciden en establecer la posibilidad de una indemnización para los afectados.

Tabla # 11 matriz definición de habeas data

ASPECTO	ECUADOR	ARGENTINA	PERU
<b>Definición de Habeas Data</b>	<p>En Ecuador, el habeas data se define como una garantía que tiene toda persona a acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales, así como a conocer el origen y finalidad de estos. Dentro de la definición Legal, La Ley Orgánica de Protección de Datos Personales de Ecuador define el hábeas data en su artículo 4 como un derecho a conocer el origen y finalidad de así mismo conocer los elementos del habeas data que comprende en los siguientes:</p> <ol style="list-style-type: none"> <li>1. Acceso. - El derecho a acceder a los datos personales que se encuentran en poder de un tercero.</li> <li>2. Rectificación. - El derecho a rectificar los datos personales que sean inexactos o incompletos.</li> <li>3. Cancelación. - El derecho a cancelar los datos personales que sean innecesarios o que hayan sido tratados de manera ilegal.</li> <li>4. Oposición: El derecho a oponerse al tratamiento de los datos personales cuando se considere que pueden afectar sus derechos fundamentales.</li> <li>5. Conocimiento del origen y finalidad: El derecho a conocer el origen y finalidad de los datos personales que se encuentran en poder de un tercero.</li> </ol>	<p>En Argentina, La Ley de Protección de Datos Personales se encuentra en Ley N° 25.326 en su artículo 1, donde se define al habeas data como una garantía al derecho que tiene toda persona a acceder, rectificar, actualizar, suprimir y oponerse al tratamiento de sus datos personales, así como a conocer el origen y finalidad. En este sentido en Argentina se comprende los siguientes elementos:</p> <ol style="list-style-type: none"> <li>1. Acceso: El derecho a acceder a los datos personales que se encuentran en poder de un tercero.</li> <li>2. Rectificación: El derecho a rectificar los datos personales que sean inexactos o incompletos.</li> <li>3. Actualización: El derecho a actualizar los datos personales que sean desactualizados.</li> <li>4. Supresión: El derecho a suprimir los datos personales que sean innecesarios o que hayan sido tratados de manera ilegal.</li> <li>5. Oposición: El derecho a oponerse al tratamiento de los datos personales cuando se considere que pueden afectar sus derechos fundamentales.</li> <li>6. Conocimiento del origen y finalidad: El derecho a conocer el origen y finalidad de los datos personales que se encuentran en poder de un tercero.</li> </ol>	<p>En Perú, el hábeas data se define como una garantía que protege derechos fundamentales que tiene toda persona. En La Ley de Protección de Datos Personales de Perú Ley N° 29733 define el habeas data en su artículo 3 como: acceder, rectificar, actualizar y suprimir sus datos personales, así como a conocer el origen y finalidad. Así mismo se adhieren a estos elementos fundamentales para esta garantía.</p> <ol style="list-style-type: none"> <li>1. Acceso: El derecho a acceder a los datos personales que se encuentran en poder de un tercero.</li> <li>2. Rectificación: El derecho a rectificar los datos personales que sean inexactos o incompletos.</li> <li>3. Actualización: El derecho a actualizar los datos personales que sean desactualizados.</li> <li>4. Supresión: El derecho a suprimir los datos personales que sean innecesarios o que hayan sido tratados de manera ilegal.</li> <li>5. Conocimiento del origen y finalidad: El derecho a conocer el origen y finalidad de los datos personales que se encuentran en poder de un tercero.</li> </ol>

**ANALISIS:** en análisis comparado de las tres legislaciones Ecuador, Argentina y Perú comparten similitudes en definiciones y elementos del habeas data, sin embargo, existen diferencias en aspectos como la legislación peruana en cuanto que no incluye la oposición de tratamiento de datos personales como elemento del habeas data, cabe mencionar que es que es de gran importancia conocer las especificidades de cada legislación para garantizar la protección de datos personales en cada país.

Elaborado por: Katherine Cornejo

Tabla # 11 matriz de legitimación activa y pasiva

ASPECTO	ECUADOR	ARGENTINA	PERU
<b>Legitimación activa</b>	<p>Ley orgánica de Garantías jurisdiccionales y control constitucional</p> <p>Art. 51 Legitimación activa. - Toda persona, natural o jurídica, por sus propios derechos o como representante legitimado para el efecto, podrá interponer una acción de hábeas data.</p>	<p>Reglamentación del proceso constitucional del habeas data ley 14.214</p> <p>ART.2 Legitimación activa. Estará legitimada para interponer esta acción toda persona física o jurídica afectada. Asimismo, están legitimados los herederos universales forzosos de la persona de la cual consten los datos, cuando la indagación tenga el propósito de defender el honor familiar.</p> <p>En el caso de afectaciones colectivas la demanda podrá iniciarla el Defensor del Pueblo de la Provincia de Buenos Aires y/o las asociaciones o grupos colectivos que acrediten legitimación</p>	<p>Código procesal peruano Ley N° 31307</p> <p>Art.55 Legitimación activa La demanda de habeas data solo puede ser ejercida por el afectado, sus tutores o curadores o por sus herederos. Cuando la demanda es interpuesta por persona jurídica de derecho privado, esta se interpone por su representante legal o por el apoderado que designe para tal efecto.</p> <p>ejemplo, en el caso de una acción de hábeas data, la legitimación activa puede corresponder al titular de los datos personales o a sus representantes legales.</p>
<b>Legitimación Pasiva</b>	<p>Art. 53 Legitimación pasiva La acción por incumplimiento procederá en contra de toda autoridad y contra de personas naturales o jurídicas particulares cuando actúen o deban actuar en ejercicio de funciones públicas, o presten servicios públicos. Procederá contra particulares también en el caso de que las sentencias, decisiones o informes de organismos internacionales de protección de derechos humanos impongan una obligación a una persona particular determinada o determinable.</p>	<p>Art.3 Legitimación pasiva. La acción procederá respecto de los titulares y/o responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes, administradores y responsables de sistemas informáticos.</p>	<p>Artículo 56. Legitimación pasiva Con la demanda se emplaza al titular o responsable y a los usuarios de bancos de datos, públicos o privados, destinados o no a proveer información.</p>

**ANALISIS:** según el análisis comparado a estos artículos sobre la legitimación activa y pasiva se concluye que los tres países tienen similitudes en cuanto a que establecen legitimación activa para el titular de los datos personales y o representantes legales, así mismo que los tres países establecen legitimación pasiva para entidades públicas, privadas personas naturales y bancos de datos, pero existe una diferencia en cuanto a que en Ecuador la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional pueden interponer la acción del habeas data en nombre de la persona titular de los datos personales, siempre y cuando cuente con su autorización expresa, en cuanto a Argentina y Perú no establece esta disposición de manera explícita, así mismo el reglamento del proceso constitucional del habeas data ley 14.214 de Argentina menciona que establece que los sucesores de las personas titular de los datos personales pueden interponer la acción del habeas data para proteger los derechos de su difunto familiar, en Ecuador y Perú no especifica esta disposición de manera explícita.

Elaborado por: katherine Cornejo

Tabla # 12 matriz comparado de procedimiento del habeas data

ASPECTO	ECUADOR	ARGENTINA	PERÚ
<ul style="list-style-type: none"> <li><b>Procedimiento</b></li> </ul>	<ul style="list-style-type: none"> <li><b>Presentación de la Acción</b> El titular de los datos personales o su representante legal presenta una acción de hábeas data ante la Agencia de Regulación y Control de la Protección de Datos Personales (ARCAD) La acción debe ser presentada por escrito y debe contener la identificación del titular de los datos personales, la descripción de los datos personales que se consideran vulnerados y la solicitud de medidas para proteger los derechos del titular</li> <li><b>Revisión y Admisión</b> La ARCAD revisa la acción presentada y verifica que cumpla con los requisitos establecidos en la ley. Si la acción es admitida, la ARCAD notifica al responsable del tratamiento de datos personales y le solicita que</li> </ul>	<ul style="list-style-type: none"> <li><b>Presentación de la Acción:</b> El titular de los datos personales o su representante legal presenta una acción de hábeas data ante la Agencia de Acceso a la Información Pública (AAIP) o ante un juez federal.</li> <li><b>Revisión y Admisión:</b> La AAIP o el juez federal revisa la acción presentada y verifica que cumpla con los requisitos establecidos en la ley.</li> <li><b>Notificación al Responsable del Tratamiento:</b> Si la acción es admitida, la AAIP o el juez federal notifica al responsable del tratamiento de datos personales y le solicita que proporcione</li> </ul>	<ul style="list-style-type: none"> <li><b>1. Presentación de la Acción:</b> El titular de los datos personales o su representante legal presenta una acción de habeas data ante la Autoridad Nacional de Protección de Datos Personales (ANPDP) o ante un juez civil.</li> <li><b>2. Revisión y Admisión:</b> La ANPDP o el juez civil revisa la acción presentada y verifica que cumpla con los requisitos establecidos en la ley.</li> <li><b>3. Notificación al Responsable del Tratamiento:</b> Si la acción es admitida, la ANPDP o el juez civil notifica al responsable del tratamiento de datos personales y le</li> </ul>

	<p>proporcione información sobre los datos personales del titular.</p> <ul style="list-style-type: none"> <li>• Investigación y Análisis La ARCAD realiza una investigación y análisis de la información proporcionada por el responsable del tratamiento de datos personales, también puede solicitar información adicional o realizar inspecciones para verificar la veracidad de la información proporcionada.</li> <li>• Resolución La ARCAD emite una resolución que puede incluir medidas para proteger los derechos del titular de los datos personales, como la rectificación, actualización o supresión de los datos personales. La resolución también puede incluir sanciones para el responsable del tratamiento de datos personales si se determina que ha vulnerado los derechos del titular.</li> <li>• Recurso de Apelación  El titular de los datos personales o el responsable del tratamiento de datos personales pueden apelar la resolución emitida por la ARCAD ante el Tribunal Constitucional.</li> <li>• Ejecución de la Resolución La ARCAD es responsable de ejecutar la resolución emitida y de verificar que se cumplan las medidas ordenadas para proteger los derechos del titular de los datos personales.</li> </ul>	<p>información sobre los datos personales del titular.</p> <ul style="list-style-type: none"> <li>• Investigación y Análisis: La AAIP o el juez federal realiza una investigación y análisis de la información proporcionada por el responsable del tratamiento de datos personales.</li> <li>• Resolución: La AAIP o el juez federal emite una resolución que puede incluir medidas para proteger los derechos del titular de los datos personales, como la rectificación, actualización o supresión de los datos personales.</li> <li>• Recurso de Apelación: El titular de los datos personales o el responsable del tratamiento de datos personales pueden apelar la resolución emitida ante la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal.</li> <li>• Ejecución de la Resolución: La AAIP o el juez federal es responsable de ejecutar la resolución emitida y de verificar que se cumplan las medidas ordenadas para proteger los derechos del titular de los datos personales.</li> </ul>	<p>solicita que proporcione información sobre los datos personales del titular.</p> <ul style="list-style-type: none"> <li>• 4. Investigación y Análisis: La ANPDP o el juez civil realiza una investigación y análisis de la información proporcionada por el responsable del tratamiento de datos personales.</li> <li>• 5. Resolución: La ANPDP o el juez civil emite una resolución que puede incluir medidas para proteger los derechos del titular de los datos personales, como la rectificación, actualización o supresión de los datos personales.</li> <li>• 6. Recurso de Apelación: El titular de los datos personales o el responsable del tratamiento de datos personales pueden apelar la resolución emitida ante la Sala Civil de la Corte Superior de Justicia.</li> <li>• 7. Ejecución de la Resolución: La ANPDP o el juez civil es responsable de ejecutar la resolución emitida y de verificar que se cumplan las medidas ordenadas para proteger los derechos del titular de los datos personales.</li> </ul>
--	--	---	---

ANALISIS: las similitudes en la presentación de la acción en los tres países el titular de los datos personales o su representante legal puede presentar una acción de habeas data ante la autoridad correspondiente, respecto a la notificación al responsable del tratamiento, en los tres países, la autoridad correspondiente notifica al responsable del tratamiento de datos personales y le solicita que le proporcione información sobre los datos personales del titular, en investigación y análisis, en los tres países, la autoridad correspondiente realiza una investigación y análisis de la información proporcionada en el tratamiento de datos y finalmente la resolución en las tres legislaciones se emite una resolución que puede incluir medidas para proteger los derechos del titular de los datos personales. Continuamente en las diferencias en Ecuador la autoridad competente es la agencia de regulación y control de datos personales ARCA, en Argentina preside la agencia de acceso a la información pública AAIP, y en Perú la autoridad nacional de protección de datos personales ANPDP, en cuanto a los plazos Ecuador y Perú coinciden con el plazo para resolver de 30 días mientras que Argentina se diferencia por el plazo de 60 días, así mismo en este contexto el recurso de apelación en Ecuador se presenta en la corte constitucional, en Argentina en la cámara de nacional de apelaciones contencioso administrativo federal y en Perú en la sala de lo civil de la corte superior de justicia. En las medidas a proteger tienen las mismas similitudes las dos legislaciones Argentina y Perú que coinciden con a suspensión o cesación del tratamiento de datos personales mientras que en Ecuador lo omiten en conclusión el procedimiento del hábeas data en Ecuador, Argentina y Perú presenta similitudes y diferencias. En general, los tres países establecen un procedimiento similar para la presentación de la acción, la notificación al responsable del tratamiento, la investigación y análisis, y la resolución. Sin embargo, existen diferencias en la autoridad competente, el plazo para resolver, el recurso de apelación y las medidas para proteger los derechos del titular de los datos personales. Es importante mencionar que cada país tiene sus propias particularidades y regulaciones en materia de protección de datos personales.

**Elaborado por: Katherine Cornejo**



Tabla # 13 matriz ámbito de aplicación del habeas data

ASPECTO	ECUADOR	ARGENTINA	PERÚ
<b>Ámbito de aplicación</b>	<p>En Ecuador, el artículo que tipifica el ámbito de aplicación del hábeas data es el artículo 4 de la Ley Orgánica de Protección de Datos Personales (LOPD), que establece lo siguiente:</p> <p>"Artículo 4.- Ámbito de aplicación</p> <p>La presente Ley es aplicable a todos los tratamientos de datos personales realizados por personas naturales o jurídicas, públicas o privadas, que se encuentren en el territorio nacional, así como a los tratamientos de datos personales realizados por personas naturales o jurídicas ecuatorianas en el extranjero.</p> <p>La presente Ley también es aplicable a los tratamientos de datos personales realizados por personas naturales o jurídicas extranjeras que se encuentren en el territorio nacional, siempre y cuando el tratamiento de datos personales se realice en el territorio nacional.</p> <p>Además, el artículo 5 de la misma ley establece que el hábeas data es aplicable a todos los datos personales, incluyendo aquellos que se encuentren en bases de datos, archivos, registros y cualquier otro medio de almacenamiento de datos.</p>	<p>El artículo que tipifica el ámbito de aplicación del hábeas data en Argentina es el artículo 43 de la Constitución Argentina, sancionado en la reforma constitucional de 1994. Este artículo establece que. Toda persona tiene derecho a la protección de sus datos personales, lo que incluye el acceso, rectificación y supresión.</p> <p>Además, la Ley de Protección de Datos Personales (Ley 25.326) también regula el ámbito de aplicación del hábeas data en Argentina. Esta ley establece que el hábeas data es aplicable a todo tratamiento de datos personales realizado por entidades públicas o privadas, incluyendo empresas, organizaciones y asociaciones</p> <p>Es importante destacar que el hábeas data en Argentina tiene un ámbito de aplicación amplio, que incluye no solo la protección de los datos personales, sino también la regulación del tratamiento de datos personales por parte de entidades públicas y privadas.</p>	<p>En Perú, el artículo que tipifica el ámbito de aplicación del hábeas data es el artículo 2 de la Ley de Protección de Datos Personales (Ley 29733), que establece lo siguiente:</p> <p>Artículo 2.- Ámbito de aplicación</p> <p>La presente Ley es aplicable a todos los tratamientos de datos personales realizados por personas naturales o jurídicas, públicas o privadas, que se encuentren en el territorio nacional, así como a los tratamientos de datos personales realizados por personas naturales o jurídicas peruanas en el extranjero.</p> <p>Además, el artículo 3 de la misma ley establece que el hábeas data es aplicable a todos los datos personales, incluyendo aquellos que se encuentren en bases de datos, archivos, registros y cualquier otro medio de almacenamiento de datos.</p> <p>Es importante destacar que el hábeas data en Perú tiene un ámbito de aplicación amplio, que incluye la protección de los datos personales y la regulación del tratamiento de datos personales por parte de entidades públicas y privadas.</p>

	Es importante destacar que el habeas data en Ecuador tiene un ámbito de aplicación amplio, que incluye la protección de los datos personales y la regulación del tratamiento de datos personales por parte de entidades públicas y privadas.		
<b>Plazos procesales</b>	30 Días Plazo	60 Días Plazo	30 Días Plazo
<b>Sanciones</b>	Penales y administrativas	Indemnización para los afectados	Indemnización para los afectados
<b>Carácter del derecho</b>	Fundamental, con énfasis en la privacidad y control sobre datos personales, es un derecho irrenunciable, imprescriptible y protegida por la ley.	Derecho constitucional y autónomo enfocado en la privacidad y protección de los datos.	Derecho fundamental que protege la autodeterminación informativa, también es irrenunciable, imprescriptible y protegido por la ley de protección de datos.

**ANÁLISIS:** El habeas data es aplicable a todos los datos personales, incluyendo, aquellos que se encuentren en base de datos, archivos, registro, y cualquier otro medio de almacenamiento de datos, así mismo los cumplen con una excepciones que establece la LOPD, como la información contenida en documentos públicos, el ámbito de aplicación del habeas data en Ecuador, Argentina, y Perú es similar, ya que todas las legislaciones establecen que el habeas data es aplicable a todos los tratamientos de datos personales realizados por personas naturales o jurídicas, públicas o privadas que se encuentren en territorio nacional, sin embargo existen exepciones al habeas data entre las tres legislaciones.

Elaborado por: Katherine Cornejo

Tabla #14 Matriz de Sujetos y Legitimación

<b>País</b>	<b>Legitimación Activa</b>	<b>Legitimación Pasiva</b>	<b>Terceros Interesados</b>	<b>Participación Ciudadana</b>
<b>Ecuador</b>	Toda persona natural o jurídica	Contra toda autoridad y contra personas naturales o jurídicas particulares	Titulares de datos personales Representantes legales Sucesores Organizaciones gubernamentales no	Participación social,
<b>Argentina</b>	Titulares del derecho o jurídica afectada, así mismos herederos universales, también podrá iniciarla los defensores públicos.	Obligados los titulares responsables y usuarios de banco de datos públicos	Intervinientes, representantes legales, sucesores	Mecanismos participativos
<b>Perú</b>	Sujetos activos, titulares, tutores, curadores o por sus herederos	Sujetos pasivos, se emplaza al titular o responsable y a usuarios de banco de datos públicos o privados.	Otros actores	Inclusión ciudadana

Elaborado por: Katherine Cornejo

## **4.2 Verificación de la idea a defender**

El habeas data en las legislaciones de Ecuador, Argentina y Perú evidencia como el derecho comparado puede ser una herramienta clave para fortalecer la protección de datos personales, armonizando las garantías procesales en América y adaptándolas a los retos tecnológicos contemporáneo, además del reconocimiento constitucional normativo uniforme, en los tres países el habeas data tiene un reconocimiento constitucional, lo que resalta su importancia como una garantía de derechos fundamentales.

En Ecuador, la Constitución de la República del Ecuador en su artículo 92 reconoce el habeas data como un recurso para acceder, ratificar o eliminar datos personales, de la misma manera en Argentina se establece en el artículo 43 de Constitución Nacional y se complementa con la ley 25.326 de Protección de Datos Personales. Por otra parte, Perú regula el habeas data en la Constitución de 1993 en su artículo 200 inciso 3 desarrollándolo mediante el Código Procesal Constitucional, esto refleja un consenso regional sobre la necesidad de proteger la autodeterminación informativa, aunque con variaciones en los procedimientos y alcances que deben ser evaluados y armonizados.

En este sentido las diferentes regulaciones en Ecuador, se reconoce los datos sensibles, pero su regulación específica se encuentra en la ley de protección de datos personales 2021, que es reciente y se encuentra en proceso de implementación. Argentina tiene una de las legislaciones más avanzadas en la región, estableciendo estrictas limitaciones al tratamiento de datos sensibles, con énfasis en el consentimiento informado y sanciones severas por el incumplimiento. De modo similar Perú incluye los datos sensibles en su Ley de Protección de datos personales N° 29733 pero enfrenta retos en la supervisión efectiva de su cumplimiento, estas diferencias permiten identificar prácticas más efectivas como el modelo argentino, que podría ser adoptada por los demás países.

En cuanto al enfoque procesal del habeas data en Ecuador el trámite del habeas data es ágil, permitiendo su interposición de manera directa ante un juez constitucional, con plazos breves para resolver. En cambio, en Argentina, su carácter procesal es robusto, con un enfoque correctivo y sancionador, especialmente contra las empresas que incumplen con la

protección de datos. Mientras que en Perú se incluye dentro del Código Procesal Constitucional, con procedimientos diseñados para garantizar celeridad, aunque enfrenta desafíos por la gestión judicial. La integración de procesos más eficientes y sanciones clara como en Argentina, puede inspirar mejoras en los sistemas ecuatoriano y peruano.

Por otra parte, dentro del impacto de las tecnologías como la TIC, la evolución tecnológica ha puesto retos similares en los tres países, como la protección de datos en la plataforma digitales o en el tratamiento masivos de datos por parte de grandes empresas. En Ecuador la ley de datos incluye aspectos relacionados con el entorno digital pero aún se encuentra en fase de consolidación. Argentina tiene una mayor trayectoria en la regulación digital y una autoridad de protección de datos activas. En cambio, Perú enfrenta desafíos en la supervisión y actualización de su legislación para adaptarse a las nuevas tecnologías. En contexto compartir experiencias y buenas prácticas mediante el derecho comparado puesto que puede ayudar a que estas legislaciones se ajusten de manera más eficaz a los desafíos contemporáneos.

Finalmente después haber analizado las doctrinas pertinentes, diversas fuentes bibliográficas y la matriz de comparación de las legislaciones de Ecuador, Argentina y Perú con relación al Estudio Comparado a las Reglas de Habeas Data, se ha corroborado la idea a defender de este trabajo investigativo si enfrenta dificultades en la protección, acceso y la privacidad de los datos de los ciudadanos, puesto que en los dos países han avanzado más en la creación de leyes específicas que regulan de manera detallada la protección y accesibilidad de datos.

## CONCLUSIONES

- Los tres países reconocen el derecho al habeas data en sus constituciones como una garantía fundamental para la protección de la privacidad y el control de los datos personales, mientras que las mismas legislaciones han desarrollado leyes específicas y detalladas para regular el tratamiento de datos personales.
- En los tres países, el habeas data garantiza a los ciudadanos el acceso, rectificación y eliminación de información personal tanto en manos del Estado como de entidades privadas, no obstante, Argentina y Perú cuentan con marcos normativos más precisos que establecen obligaciones específicas para los procesadores de datos, como el consentimiento informado y medidas de seguridad, mientras que en Ecuador la normativa es más general y menos detallada en cuanto a las obligaciones de los responsables de datos.
- Los procesadores de datos están obligados a garantizar la confidencialidad y seguridad de los datos en los tres países, Ecuador Argentina y Perú así mismo cuentan con normativas más estrictas que especifican sanciones para el incumplimiento, incluyendo multas y responsabilidades civiles, aunque existe responsabilidad sobre el manejo de datos.
- Tanto en Argentina como en Perú, existen autoridades especializadas que supervisan el cumplimiento de las normativas de protección de datos y aplican sanciones a los infractores, lo que refuerza el cumplimiento del habeas data, en Ecuador, aunque hay normas que protegen el derecho a la privacidad, la ausencia de un organismo dedicado a la protección de datos personales limita el control y las sanciones en comparación con los otros dos países.

## RECOMENDACIONES

- Se recomienda fortalecer la capacitación continua a los funcionarios públicos y entidades privadas en los tres países para asegurar una aplicación coherente y efectiva del derecho al hábeas data, esto incluye ofrecer talleres, seminarios y guías prácticas sobre los principios de protección de datos personales y el procedimiento del hábeas data, al mejorar el conocimiento y la comprensión de esta garantía constitucional, se facilita una respuesta más eficiente y uniforme ante las solicitudes de acceso, rectificación y eliminación de datos, sin necesidad de reformar las leyes existentes.
- Se sugiere implementar protocolos y guías prácticas en Ecuador que detallen las mejores prácticas para el tratamiento de datos personales, alineándose con los estándares de Argentina y Perú, estos protocolos pueden incluir procedimientos específicos para garantizar el consentimiento informado y medidas de seguridad adecuadas, mejorando así la aplicación del hábeas data, además, la capacitación regular de los responsables del manejo de datos contribuirá a un mayor cumplimiento de las obligaciones y a la protección efectiva de los derechos de los ciudadanos, sin necesidad de modificar el marco legal vigente.
- Se recomienda que las autoridades encargadas de la protección de datos en Ecuador, Argentina y Perú fortalezcan los mecanismos de supervisión y auditoría para garantizar que los procesadores de datos cumplan con las obligaciones de confidencialidad y seguridad, esto puede lograrse mediante inspecciones regulares, auditorías independientes y el fomento de la autoevaluación por parte de las entidades, así como campañas de concienciación sobre las sanciones existentes por incumplimiento, de esta manera, se incentivará un manejo adecuado de los datos personales y se reducirá el riesgo de infracciones, sin necesidad de modificar las leyes vigentes.
- Promover campañas educativas para informar a la ciudadanía, empresas sobre sus derechos y obligaciones en materia de protección de datos puede mejorar el cumplimiento sin necesidad de crear nuevas entidades.

## **BIBLIOGRAFÍA**

- Arce, F. (2009). *El Habeas Data como Garantía jurisdiccional e instrumento efectivo de Garantía del Derecho a la privacidad en la Legislacion Ecuatoriana*. Universidad del Azuay, Cuenca.
- Arias, F. (2006). *El proyecto de investigacion introduccion a la metodologia cientifica*. Caracas: Editorial Episteme.
- Asamblea Nacional. (2009). *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*.
- Byron Villagómez Moncayo, G. V. (2014). *El hábeas data y la nueva regla jurisprudencial de la Corte Constitucional*.
- Byron Villagómez Moncayo, G. V. (2014). *El hábeas data y la nueva regla jurisprudencial de la Corte Constitucional: la prescindencia de la demostración de daño o perjuicio para la procedencia de la acción*.
- Cabanellas, G. (2006). *Diccionario Jurídico Elemental*. Buenos Aires.
- Castillo, C., & Reyes, B. (2015). *Guia metodologica de proyectos de investigacion social*. Editorial Upse.
- Chanamé Orbe, R. (s.f.). *Hábeas data y el derecho fundamental a la intimidad de la persona*. 2003. Universidad Nacional Mayor de San Marcos., Lima.
- Chiriboga Zambrano, G. (2001). *La acción de amparo y de hábeas data: garantías de los derechos constitucionales y su nueva realidad jurídica*. Quito: AAJ - ILDIS.
- Constitución Política del Perú . (1993). En *Constitución Política del Perú* .
- Contreras, P. (2020). El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa. En P. Contreras, *Habeas Data* (pág. 56).



- De Pina Vara, R. (2008). *Diccionario de Derecho*. ed. Porrúa.
- Enrique, P.-L. R. (2017). *El procedimiento de Habeas Data*. Madrid: Dykinson.
- Falcón, E. (2021). *Proteccion de datos y el Habeas Data*.
- Flores Dapkevicius, R. (2011). *Amparo, Hábeas Corpus y Hábeas Data*. Buenos Aires: Editorial B de F.
- Flores Polo, P. (1978). *Diccionario de terminos jurídicos*. Lima: Marsol Editores.
- Garate. (2021). Ecuador y el sistema de protección de derechos humanos de la ONU. *Tercera Edición revisada de 1000 ejemplares*.
- Garate. (2021). ECUADOR Y EL SISTEMA DE PROTECCIÓN DE DERECHOS HUMANOS DE LA ONU. *Tercera Edición revisada de 1000 ejemplares*.
- Gárate Amoroso, J., Reina Cunín, J., Samaniego Nugra, E., & Loyola Moreano, K. (2021). Habeas Data: origen y evolución. *Revista Lex*, 4, 197-210. doi:<https://doi.org/10.33996/revistalex.v4i13.82>
- García. (2006). La acción de hábeas data en la constitución de 2008: análisis jurídico y jurisprudencial. *tesis*, 134.
- Guanín-Collaguazo, O. (2024). El habeas data como garantía de protección al derecho a la intimidad. *Revista Científica De Ciencias Humanas Y Sociales RECIHYS*, 2(1), 20-25. doi:<https://doi.org/10.24133/recihys.v2i1.3472>
- Ley Orgánica de Protección de Datos Personales. (2021). En *Ley Orgánica de Protección de Datos Personales* (pág. 70).
- Machuca, S. (2018). Reglas del habeas data. En M. S. Vinueza, *Reglas del habeas data*.
- MASCIOTRA, M. (2004). *Naturaleza jurídica del habeas data*.

- Ordóñez Pineda, L. (2019). El hábeas data como garantía procesal frente a las tecnologías de la información y comunicación: situación en el contexto ecuatoriano. *RES NON VERBA REVISTA CIENTÍFICA*, 9, 9(2), 1-14.
- Pacheco, J. M. (2014). Real academia Española. En J. M. Pacheco, *Real academia Española*.
- Pauner, C. (2014). *Derecho a la información*. Valencia: Tirant Lo Blanch.
- Perez. (2017). el hábeas data como garantía procesal. En Perez, *el hábeas data como garantía procesa* (pág. 128).
- Pérez, E. C. (2017). El procedimiento de habeas data. En E. C. Pérez, *El procedimiento de habeas data*.
- Quíroz Papa de García, R. (2016). El Hábeas Data, protección al derecho a la información. *Letras (online)*, vol.87, 14. Obtenido de [http://www.scielo.org.pe/scielo.php?script=sci\\_arttext&pid=S2071-50722016000200002&lng=es&nrm=iso](http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2071-50722016000200002&lng=es&nrm=iso)
- Troncoso. (2010). *el hábeas data como garantía procesal*.
- Vizcaino Barba, F. (2015). *La acción de hábeas data en la constitución de 2008: análisis*. Universidad Andina Simón Bolívar, Quito.
- Zavala, J. (2010). *Derecho constitucional*.