

# UCUENCA

## Universidad de Cuenca

Facultad de Jurisprudencia y Ciencias Políticas y Sociales

Carrera de Derecho

**Análisis Comparativo a partir de los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales del Comité Jurídico Interamericano y los Principios de la Ley Orgánica de Protección de Datos Personales**


Trabajo de titulación previo a la obtención del título de Abogado de los Tribunales de la República del Ecuador y Licenciado en Ciencias Políticas y Sociales

**Autor:**

Juan Francisco Lara Santana

**Director:**

Diego Andrés Monsalve Tamariz

ORCID:  0000-0002-4207-0766

**Cuenca, Ecuador**

2023-10-16

## Resumen

Ecuador aprobó en 2021 la Ley Orgánica de Protección de Datos Personales que tiene como objeto garantizar el derecho a la protección de datos de carácter personal que, hasta aquel entonces no contaba con una normativa específica. Paralelamente, el Comité Jurídico Interamericano publica los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales en aras de armonizar las iniciativas legislativas de los Estados Miembro de la Organización de Estados Americanos. Esta investigación tiene como objetivo analizar los principios establecidos en ambos instrumentos y evidenciar la influencia de los instrumentos internacionales en la normativa nacional.

*Palabras clave:* principios jurídicos, protección de datos, derecho a la privacidad



El contenido de esta obra corresponde al derecho de expresión de los autores y no compromete el pensamiento institucional de la Universidad de Cuenca ni desata su responsabilidad frente a terceros. Los autores asumen la responsabilidad por la propiedad intelectual y los derechos de autor.

**Repositorio Institucional:** <https://dspace.ucuenca.edu.ec/>

### Abstract

Ecuador approved in 2021 the Organic Law of Personal Data Protection with the purpose of guaranteeing the right to personal data protection that, until that moment, was not regulated by a specific legal body. Simultaneously, the Interamerican Juridical Committee published the Updated Principles on Privacy and Personal Data Protection as an initiative to harmonize the legislative initiatives of the Member States of the Organization of American States. This research intends to analyze the principles established in both bodies and evidence the influence of international instruments in national law.

*Keywords:* legal principles, data protection, right to privacy



The content of this work corresponds to the right of expression of the authors and does not compromise the institutional thinking of the University of Cuenca, nor does it release its responsibility before third parties. The authors assume responsibility for the intellectual property and copyrights.

**Institutional Repository:** <https://dspace.ucuenca.edu.ec/>

## Índice de contenido

Índice de contenido.....	4
Dedicatoria.....	6
Agradecimientos.....	6
Capítulo I Antecedentes históricos de la protección de datos en el ámbito nacional e internacional. ....	7
1.1.    Génesis de la protección de datos en el mundo occidental.....	7
1.1.1.    Estados Unidos de América.....	7
1.1.2.    Reino de España.....	8
1.1.3.    República de Colombia.....	9
1.2.    Evolución histórica del derecho a la protección de datos en la legislación ecuatoriana previa a la Constitución de Montecristi .....	11
Capítulo II Contexto internacional del Estado Ecuatoriano sobre la protección de datos personales y marco constitucional del derecho a la protección de datos.....	14
2.1.    Estatus del Ecuador en el Sistema Internacional (Organización de las Naciones Unidas) .....	14
2.2.    Estatus del Ecuador en el contexto Iberoamericano (Red Iberoamericana de Protección de Datos) .....	17
2.3.    Marco Constitucional del derecho a la protección de datos personales .....	22
Capítulo III Análisis comparativo entre los Principios Actualizados sobre Privacidad y la Protección de Datos Personales del Comité Jurídico Interamericano de la Organización de Estados Americanos y la Ley Orgánica de Protección de Datos Personales del Ecuador ....	25
3.1.    Análisis del listado de Principios Actualizados sobre la Privacidad y la Protección de Datos Personales de la OEA.....	25
3.1.1.    Principio Uno. – Finalidades Legítimas y Lealtad.....	26
3.1.2.    Principio Dos. – Transparencia y consentimiento .....	27
3.1.3.    Principio tres. – Pertinencia y Necesidad .....	28
3.1.4.    Principio cuatro. – Tratamiento y conservación limitados .....	28
3.1.5.    Principio cinco. – Confidencialidad.....	29
3.1.6.    Principio seis. – Seguridad de los Datos .....	29
3.1.7.    Principio siete. – Exactitud de los Datos.....	30
3.1.8.    Principio ocho. – Acceso, Rectificación, Cancelación, Oposición y Portabilidad.	31
3.1.9.    Principio nueve. – Datos Personales sensibles.....	33

3.1.10. Principio diez. – Responsabilidad.....	33
3.1.11. Principio once. – Flujo transfronterizo de Datos y Responsabilidad.....	35
3.1.12. Principio doce. – Excepciones.....	36
3.1.13. Principio trece. – Autoridades de Protección de Datos.....	37
3.2. Análisis del listado de principios establecidos en la Ley Orgánica de Protección de Datos Personales.....	37
3.2.1. Principio de juridicidad.....	38
3.2.2. Principio de lealtad.....	39
3.2.3. Principio de Transparencia.....	40
3.2.4. Principio de finalidad.....	40
3.2.5. Principio de pertinencia y minimización de datos personales.....	41
3.2.6. Principio de Proporcionalidad del tratamiento.....	41
3.2.7. Principio de confidencialidad.....	42
3.2.8. Principio de calidad y exactitud.....	42
3.2.9. Principio de Conservación.....	43
3.2.10. Principio de seguridad de datos personales.....	44
3.2.11. Principio de responsabilidad proactiva y demostrada.....	45
3.2.12. Principio de Aplicación Favorable al Titular.....	46
3.2.13. Principio de Independencia del Control.....	47
3.3. Conclusiones.....	47
3.4. Críticas y recomendaciones.....	48
Referencias.....	50

## **Dedicatoria**

A mis padres y mi hermano, símbolos de perseverancia, fortaleza y dedicación.

## **Agradecimientos**

A la Universidad de Cuenca, por ser sede de excelencia académica y darme la oportunidad de ponerme al servicio de la justicia y la sociedad.

## **Análisis Comparativo a partir de los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales del Comité Jurídico Interamericano y los Principios de la Ley Orgánica de Protección de Datos Personales.**

### **Capítulo I**

#### **Antecedentes históricos de la protección de datos en el ámbito nacional e internacional.**

##### **1.1. Génesis de la protección de datos en el mundo occidental.**

El origen de la protección de datos personales en la sociedad es un fenómeno que se ha desarrollado a lo largo de varias décadas y en varios estados, por lo que es importante analizar los hitos que se han dado en relación a este derecho a nivel internacional, con mayor precisión en las Américas y Europa. De ahí que es menester determinar los momentos que marcaron las primeras nociones de lo que en la actualidad se conoce como el derecho a la protección de datos en tales regiones, teniendo como referencia a Estados Unidos, España como referente de Europa y el vecino país de Colombia.

##### **1.1.1. Estados Unidos de América. –**

En Estados Unidos de América se origina las modernas nociones del derecho a la intimidad desde el concepto de “privacy” o privacidad. En el artículo “The Right to Privacy” publicado por los autores Samuel D. Warren y Louis D. Brandeis en Harvard Law Review, se aborda por primera vez lo que modernamente se conoce como el derecho a la intimidad. (Warren & Brandeis, 1890)

En este artículo se desarrollan las bases legales relacionadas al “derecho a la soledad” (right to be let alone) que fue abordado con antelación en “The elements of Torts” del Juez Thomas McIntyre Cooley, y nació con la intención de establecer límites jurídicos a la intromisión en la vida privada de las personas como concomitancia a la actividad intrusiva de la prensa y a los avances tecnológicos de la época. Este artículo aborda como dichos avances podrían generar intromisiones en el fuero privado de las personas, sin que éstas tengan la posibilidad de contar con una reparación legal por aquello.

Posteriormente y, como sucede usualmente en los países con sistemas anglosajones, el derecho a la privacidad tuvo un desarrollo jurisprudencial muy amplio. A partir del aporte doctrinario de Warren Y Brandeis, el derecho a la privacidad se transformó de una noción aislada de la Academia a un derecho autónomo que derivó en el reconocimiento de otros derechos accesorios como el derecho al honor, la inviolabilidad del domicilio y, evidentemente, el derecho a la protección de datos personales. (González Porras, 2015)

## **1.1.2. Reino de España. –**

Los primeros indicios en la normativa sobre protección de datos en España se remontan al origen de la Constitución de 1980. En los debates parlamentarios que se llevaron en 1978 los legisladores expresaron su interés en plasmar en el texto constitucional que se encuentra hoy vigente el limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos (Spain, 2018). Estas propuestas fueron incorporadas en la norma fundamental de España después de un referéndum y la sanción del Rey de España el 27 de diciembre de 1978.

La legislación española sobre protección de datos personales fue desarrollada más de una década después que las garantías constitucionales previamente mencionadas, pues a partir del año 1992 España encuentra camino legal para regular este derecho con la Ley 5/1992 a través de la cual se crea la Agencia de Protección de Datos, el Registro Público de ficheros informáticos, esta Ley, en palabras de Clímaco Valiente, dio un andamiaje procedimental garante y respetuoso de la libertad informática, protección de datos personales o autodeterminación informativa. (Clímaco Valiente, 2012)

Durante este periodo entre la garantía constitucional al honor y la intimidad personal, y la carencia de legislación nacional que de eficacia a dicha garantía, este derecho fue materializado mediante la aplicación e invocación de instrumentos internacionales de protección de datos personales por el Tribunal Constitucional en procesos de amparo constitucional (el de mayor relevancia el Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal de 1981, Convenio 108) e indirectamente a través de la Ley Orgánica de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen de 1982, pero como Clímaco Valiente comenta, ésta resultó insuficiente para abarcar los avances tecnológicos ya en aquel entonces, además que su objeto de protección no era el mismo que nacía en Europa.



Sin embargo, para 1992 España finalmente cuenta con una ley que formalmente regula el derecho a la protección de datos personales, tal ley es la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, también llamada LORTAD. Esta ley se promulga cumpliendo el mandato constitucional del artículo 18.4 que, durante más de catorce años, quedó al amparo de los convenios internacionales y la aplicación del Tribunal Constitucional. (LORTAD, 1992)

España, al ser miembro de la Comunidad Europea y Estado Parte del Acuerdo de Schengen de 1985, participa en el intercambio de información entre los estados del espacio común para fines policiales y de seguridad a través del Sistema de Información Schengen. En el Acuerdo se establece que los estándares mínimos de protección de información debían ser los del Convenio 108. (Clímaco Valiente, 2012)

### **1.1.3. República de Colombia. –**

Los primeros indicios de protección de datos personales en el ordenamiento jurídico colombiano son gestados en la Constitución Política de 1991, en cuyo artículo 15 se establece lo siguiente:

ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. (Constitución Política de Colombia, 1991)

Como se ha evidenciado en el caso estadounidense, la protección de datos personales es, en sus orígenes, accesoria al derecho a la intimidad hasta que su desarrollo es tal que deviene un derecho fundamental autónomo. Algo que destaca Rojas Bejarano es que, a partir de este precepto constitucional se originan a su vez los derechos de intimidad, buen nombre y, evidentemente, la protección de datos. (Rojas Bejarano, 2014)

Para 2006, la Ley de Habeas Data regula el manejo de la información contenida en bases de datos personales con un especial énfasis en información financiera, crediticia, comercial, de servicios y la proveniente de terceros, adicionalmente, esta norma se orientó mediante dos decretos reglamentarios expedidos en los años 2009 (Decreto 1727) y 2010 (Decreto 2952).

A través de esta norma se instituye una delegatura dependiente de la Superintendencia de Industria y Comercio para el control y regulación de la materia normada en mencionada norma; así como la creación del Registro Nacional de Bases de Datos cuya administración compete a esta entidad pública. (Ley 1266 de 2008, 2008)

La jurisprudencia colombiana ha tenido un desarrollo paralelo a los preceptos normativos, de los cuales se puede destacar diez sentencias que recopilan varios conceptos e instituciones relativas a la protección de datos. La jurisprudencia colombiana ha ilustrado magistralmente dichos conceptos e instituciones, por lo que es menester sintetizar el desarrollo conferido por estos de las cuales destacan las siguientes:

1. Sentencia T-414 de 1992. – Analiza la intimidad personal y familiar en contraposición con el derecho a la información, se protege la intimidad como una forma de asegurar la paz y tranquilidad que exige el desarrollo físico, intelectual y moral de las personas como derecho constitutivo de la personalidad. (Sentencia No. T-414/92, 1992)
2. Sentencia SU-082 de 1995. – Analiza el conflicto existente entre el derecho al buen nombre y el derecho a la información cuando existe divulgación de información. El derecho a la información se limita a existir cuando la misma sea veraz, no existe derecho a la información que no es cierta ni para la información incompleta. La Corte Constitucional de Colombia considera que, en el caso del buen nombre, este no se ve vulnerado cuando la difusión o acceso a la información es veraz, en todo caso lo reafirma, por apegarse a la verdad. (Sentencia No. SU-082/95, 1995)
3. Sentencia T-729 de 2002. – Esta sentencia aborda el ámbito de operatividad del derecho a la autodeterminación informática en la integridad del contexto material: Objeto o actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos. (Sentencia T-729/02, 2002)
4. Sentencia C-334 de 2010. – Esta sentencia provee los escenarios en los que se administra acceso a la información y sus diversos caracteres, como en el caso de la información pública (acceso sin reserva y sin que se requiera autorización para ello), información semiprivada (acceso por orden de autoridad judicial o administrativa), información privada (acceso únicamente por autoridad judicial), información reservada (sometida a la reserva propia del proceso penal, cuyo interés le compete únicamente

al titular a que está estrechamente relacionada con la protección de sus derechos a la dignidad humana). (Sentencia C-334/10, 2010)

5. Sentencia C-748 de 2011. – Esta sentencia se analiza el concepto y las líneas interpretativas del derecho al habeas data en la jurisprudencia constitucional. En ello, se determina que este derecho tiene las siguientes prerrogativas mínimas:

El derecho de las personas a conocer –acceso- la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; 2) el derecho a incluir nuevos datos con el fin de que se provea una imagen completa del titular; 3) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; 4) el derecho a que la información contenida en bases de datos sea rectificadas o corregidas, de tal manera que concuerde con la realidad; 5) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa. (Sentencia C-748/11, 2011)

Una vez analizado el desarrollo histórico que ha tenido el derecho a la protección de datos en estas tres jurisdicciones, resulta evidente que el desarrollo de este derecho nace a partir del derecho a la intimidad, siendo este el caso de Estados Unidos, España y Colombia, para consecuentemente surgir como un derecho fundamental autónomo, cuyo desarrollo no se limita al ámbito legislativo, si no que éste ha dado, a nivel constitucional en el caso de España y Colombia, los pilares básicos para una protección mucho más integral y coherente con los ordenamientos jurídicos a través de la jurisprudencia y la interpretación de los tribunales constitucionales de ambos países, mientras que Estados Unidos presenta un caso muy particular, pues su primer indicio y fuente de inspiración para la protección en su sistema anglosajón fue el aporte doctrinario de Warren y Brandeis.

## **1.2. Evolución histórica del derecho a la protección de datos en la legislación ecuatoriana previa a la Constitución de Montecristi.**

La Ley Orgánica de Protección de Datos Personales constituye el primer instrumento propio cuya finalidad es garantizar el efectivo ejercicio del derecho a la protección de datos personales consagrado en la Constitución del Ecuador de 2008. Previo a esta Ley, la protección de datos personales constituía un precepto constitucional cuyo desarrollo pedía urgentemente la incorporación de normativa específica para esta materia. Resulta

inconcebible que para un derecho constitucionalmente protegido como este no exista protección jurídica especializada en la materia y que sea apropiada para el contexto tecnológico e informático actual.

A partir de la Constitución de Montecristi, el Ecuador protege el derecho a la protección de datos personales como establece el artículo 66 numeral 19 cuyo texto prescribe lo siguiente:

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

(...) 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.  
(Constitución de la República del Ecuador, 2008)

Aunque este precepto resulta fundamental para comprender el contexto jurídico normativo de la protección de datos personales en Ecuador, la primera aproximación a esta institución jurídica se remonta a la Constitución de 1976, misma que en el año 1996 tuvo algunas reformas, entre ellas, la incorporación de la garantía jurisdiccional del habeas data. El texto constitucional de aquel entonces establecía en el artículo 30 lo siguiente:

Art. 30.- Toda persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre si misma o sobre sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su finalidad.

Igualmente, podrá solicitar ante el funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquellos si fueren erróneos o afectaren ilegítimamente sus derechos.

Se exceptúan los documentos reservados por razones de seguridad nacional.  
(Constitución Política de la República del Ecuador, 1996)

En el Registro Oficial No. 99 del 2 de julio de 1997 se publica la Ley de Control Constitucional a través de la cual se establece el recurso de hábeas data como un mecanismo para tener acceso a documentos, bancos de datos e informes sobre las personas o sus bienes, que se encuentren el poder de entidades públicas, personas naturales o jurídicas privadas, esto incluye conocer el uso y finalidad de la información contenida en ellos. A través de esta Ley, Ecuador cuenta por primera vez con un mecanismo legal para poder ejercer el derecho al acceso, actualización, rectificación, eliminación o anulación de información personal. (Ley de Control Constitucional, 1997)

Esta Ley tuvo ciertas modificaciones y reformas que permitieron que la misma se adapte al contexto constitucional de 1998 con la vigencia de una nueva constitución política, algunas referentes al Tribunal Constitucional que se establecía a través de este instrumento. En referencia al hábeas data como garantía constitucional en 1998 éste estaba recogido en el artículo 94 de dicha carta magna, cuyo texto establecía lo siguiente:

Artículo 94.- Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito.

Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.

Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización.

La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional. (Constitución Política de la República del Ecuador, 1998)

Adicionalmente, la Constitución de 1998 reconocía y garantizaba el derecho a la intimidad como un derecho civil consagrado en el artículo 23 numeral 8, este derecho era reconocido tanto en la esfera individual como un derecho de intimidad familiar. El mandato de este derecho incluye la protección legal del nombre, la imagen y la voz de la persona. Paralelamente, el artículo 23 mandaba al Estado a reconocer y garantizar la inviolabilidad y el secreto de la correspondencia y de cualquier otro tipo o forma de comunicación, su retención, apertura y examinación solo estaba permitida los casos previstos en la ley.

Como Naranjo Godoy señala, el derecho a la protección de datos personales es antecedido por el derecho a la intimidad (Naranjo Godoy, 2021), este proceso de génesis del derecho a la protección de datos personales ya ha sido resaltado en la configuración jurídico normativa en los casos de Estados Unidos y España, consecuentemente es fundamental comprender y analizar el precedente histórico de la evolución del derecho a la intimidad en Ecuador, aún si previo a la constitución del 2008 no era un derecho que haya sido recogido de manera individual en la norma fundamental de la República.

## Capítulo II

### Contexto internacional del Estado Ecuatoriano sobre la protección de datos personales y marco constitucional del derecho a la protección de datos.

#### 2.1. Estatus del Ecuador en el Sistema Internacional (Organización de las Naciones Unidas).

La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos resalta la importancia que tiene el goce del derecho a la privacidad para la realización de otros derechos fundamentales como las libertades de expresión, asociación, pero no sólo se limita al goce de derechos de primera generación si no que la plena vigencia de la privacidad como derecho fundamental también permite ejercer derechos económicos, sociales y culturales. (Office of the United Nations High Commissioner for Human Rights, 2023)

Ecuador, como Estado Miembro de la Organización de las Naciones Unidas, participa activamente en la adopción y cumplimiento de los estándares que las distintas dependencias, a tal punto que en reiteradas ocasiones ha sido elegido para formar parte del Consejo de Seguridad de las Naciones Unidas y en su momento fue reconocido como el primer Estado Miembro en ratificar los 27 tratados de la ONU en materia de derechos humanos. Resulta lógico que el progreso continuo en los lineamientos de protección de derechos fundamentales en la ONU es muy útil como punto de referencia en lo que concierne a la adopción de políticas públicas de protección de datos personales y, en el caso de los convenios y tratados de carácter obligatorio, determinan el desarrollo normativo de la materia en cuestión. (Ministerio de Relaciones Exteriores y Movilidad Humana, 2020)

En lo que concierne a tratados y convenios internacionales del sistema universal que vinculen al derecho a la protección de datos personales como consecuencia del derecho a la privacidad destaca el artículo 12 de la Declaración Universal de Derechos Humanos, en este se establece que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.” (Declaración Universal de Derechos Humanos, 1948). Como se ha evidenciado con antelación, la protección de la privacidad es el antecedente de la protección de datos personales que responde a las necesidades contemporáneas de la sociedad moderna.

La privacidad y la protección de datos personales no son un concepto extraño en la ONU, pues existen varias resoluciones adoptadas a nivel de la Asamblea General y del Consejo de Derechos Humanos en vinculados a la materia. Entre varias, las que más destacan son tres: La primera siendo la Resolución de la Asamblea General 5/95 del 14 de diciembre de 1990 en la que se establecen los principios rectores sobre la reglamentación de los ficheros computarizados de datos personales. A través de esta resolución se aprueban los principios que a su vez fueron establecidos en la resolución 1990/38 del Consejo Económico y Social, estos principios establecen lo siguiente:

1. Principio de licitud y lealtad. – Se refiere a la recolección y utilización lícitos de la información relativa a las personas, alineados a los propósitos y principios establecidos en la Carta de la ONU.
2. Principio de exactitud. – Obligación de verificar la exactitud y pertinencia de los datos en los ficheros para evitar errores por omisión, la obligación de actualizar periódicamente los datos por parte del encargado de los datos.
3. Principio de finalidad. – La finalidad de un fichero y su utilización deben especificarse y justificarse, adicionalmente deben ser publicitados o ponerse en conocimiento de la persona interesada para asegurar que todos los datos sigan siendo pertinentes en función de la finalidad perseguida, que ningún dato sea revelado o utilizado sin consentimiento del titular, y que el periodo que se conservan los datos no exceda el necesario para alcanzar la finalidad con la que han sido registrados.
4. Principio de acceso de la persona interesada. – Toda persona que demuestre su identidad tiene derecho a saber si se procesa información concerniente a ella (...) a rectificar o suprimir tal información cuando sus registros son ilícitos, injustificados o inexactos.
5. Principio de no discriminación. – Este principio prevé que la información contenida en los ficheros no debería contener registros que puedan acarrear discriminación ilícita o arbitraria, particularmente información sobre origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o sobre asociaciones o afiliaciones sindicales.
6. Facultad de establecer excepciones. – Pueden establecerse excepciones a los principios 1 a 4 siempre que respondan a la necesidad de proteger la seguridad nacional, orden público, salud o moral pública y, particularmente los derechos y libertados de los demás en especial las personas perseguidas. Estas excepciones deben estar establecidas en la ley o una reglamentación equivalente y adoptada a través del mecanismo previsto en el sistema jurídico nacional. Para las excepciones relativas al principio 5, estas deben estar



sujetas a los mismos presupuestos establecidos para los principios 1 a 4 y sólo podrán establecerse en el marco de los límites previstos en la Carta Internacional de Derechos Humanos y los instrumentos pertinentes en materia de protección de derechos humanos y lucha contra la discriminación.

7. Principio de seguridad. – Este principio se refiere a la adopción de medidas que protejan los ficheros de riesgos naturales, como pérdida accidental o destrucción por accidentes, así como riesgos humanos como accesos sin autorización, utilización clandestina de datos o daño por virus informáticos.
8. Control y sanciones. – Consiste en la designación de una autoridad que esté amparada en el orden jurídico del Estado que se encargue del control del resto de principios, esta autoridad debe ser un organismo técnico, imparcial e independiente de las personas u organismos encargados del procesamiento de datos.
9. Flujo transfronterizo de datos. – Este principio alude a la compatibilidad de las garantías entre estados, pues cuando dos estados ofrezcan garantías de protección similares, los datos pueden circular tan libremente como en el interior de cada uno de los territorios respectivos. Cuando estas garantías no sean compatibles, no se pueden imponer medidas restrictivas a la circulación de datos a no ser que ésta resulte imperativa para la protección de la vida privada.
10. Campo de aplicación. – Algo que la resolución contempló en aquel entonces es la aplicación obligatoria en los ficheros computarizados y la aplicación facultativa en ficheros físicos y a ficheros que contengan información de personas jurídicas, con especial énfasis en personas jurídicas que tengan en su posesión información de personas naturales. (General Assembly Resolution 45/95, Guidelines for the regulation of computerized personal data files, 1990)

Esta resolución resulta de vital importancia en el nacimiento de la Ley Orgánica de Protección de Datos Personales, pues precisamente fue uno de los antecedentes que el legislador tomó en consideración para la promulgación de dicha norma y la formulación de los estándares vigentes en dicha norma, mismos que serán analizados en otro capítulo. Como se puede evidenciar, la resolución 45/95 de la Asamblea General de la ONU es el primer precedente de una organización intergubernamental que ilustra a los estados miembros las directrices apropiadas para una efectiva protección de datos almacenados en ficheros computarizados.

La segunda resolución de gran relevancia se destaca en relación al derecho a la privacidad en la era digital. La ONU ha aprobado varias resoluciones enfocadas a la misma desde la perspectiva de la privacidad como un derecho humano que debe estar protegido a su vez en Internet. En 2015, el Consejo de Derechos Humanos de la ONU aprobó a través de la



resolución 28/16 la designación de un relator especial para la materia que se encargue de reunir información sobre los marcos nacionales e internacionales, las prácticas, estudio de tendencias y retos relacionados al derecho a la privacidad y que; entre otras funciones, se encargue a su vez de formular recomendaciones para garantizar la protección del mismo en las esferas analizadas. En general, el rol de este relator es del participar activamente en la promoción de políticas que promuevan la defensa y promoción del derecho a la privacidad en Internet (Resolution 28/16. The right to privacy in the digital age, 2015).

La tercera resolución destacada en Naciones Unidas es la resolución 68/167 de la Asamblea General. A través de esta resolución que fue aprobada en 2013, la ONU hace un llamado a sus Estados Miembros a respetar y proteger el derecho a la privacidad, esto incluye el contexto de la comunicación digital, así como a tomar medidas legislativas y de otra índole para dar alto a las vulneraciones de derechos en la materia. Además, la resolución 68/167 exhorta a los estados a efectuar revisiones a los mecanismos que cada Estado cuenta para supervisar comunicaciones, interceptar y recolectar datos personales de tal manera que prevalezca el derecho a la privacidad y la eficacia y vigencia absoluta de las obligaciones de los estados en relación con los instrumentos internacionales de derechos humanos. Finalmente, esta resolución solicita al Alto Comisionado de Derechos Humanos la emisión de un reporte sobre la protección del derecho a la privacidad en el contexto de la supervisión local e internacional, la interceptación de comunicaciones y la recolección de datos personales, incluyendo datos e información a escala masiva, emitiendo también recomendaciones a considerar por los Estados Miembros. (General Assembly Resolution 68/167. The right to privacy in the digital age, 2013)

## **2.2. Estatus del Ecuador en el contexto Iberoamericano (Red Iberoamericana de Protección de Datos).**

La Red Iberoamericana de Protección de Datos (RIPD) nace en el marco del Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua, Guatemala del 1 al 6 de junio de 2003, esta iniciativa surge a partir de la XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos en Santa Cruz, Bolivia en 2003. Esta red funciona como un mecanismo de integración para el desarrollo de iniciativas y proyectos vinculados con la protección de datos. La RIPD ha fomentado desde su establecimiento la promoción de desarrollo normativo necesario para garantizar eficazmente el derecho a la protección de datos personales, lo que ha concluido que se hayan promulgado leyes generales de

protección de datos personales en diez estados miembros. (Red Iberoamericana de Protección de Datos, 2023)

En palabras de la propia Red, uno de los hitos fundamentales que se logró a través de los procesos regulatorios en la región fue la adopción de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Red Iberoamericana de Protección de Datos, 2020). Estos fueron aprobados en 2017 como consecuencia de la XXI Cumbre Iberoamericana de Jefes de Estado y de Gobierno celebrada en Colombia. Éstos cumplen varios objetivos, entre los que destacan el establecer un conjunto de principios y derechos comunes de protección de datos personales para el desarrollo de legislación nacional con reglas homogéneas en la región, garantizar la tutela del derecho a la protección de datos mediante reglas comunes que aseguren el debido tratamiento de los mismos, facilitar el flujo de datos entre estados iberoamericanos y coadyuvar el crecimiento económico y social; y favorecer la cooperación internacional entre las autoridades de control designados en cada estado, con otras autoridades de control no pertenecientes a la región y organismos internacionales en la materia (Red Iberoamericana de Protección de Datos, 2017).

Los principios de protección de datos personales son los siguientes:

1. Principio de Legitimación. – El responsable por regla general solo puede tratar datos personales cuando se presente en alguno de los siguientes supuestos:
  - a. El titular otorgue su consentimiento con finalidad específica;
  - b. El tratamiento es necesario para cumplir una orden judicial, resolución o mandato fundado y motivado por autoridad pública competente;
  - c. El tratamiento es necesario para el ejercicio de las facultades de las autoridades públicas o se realice en virtud de una habilitación legal;
  - d. El tratamiento es necesario para la defensa de los derechos del titular;
  - e. El tratamiento es necesario para el cumplimiento de un contrato precontrato del que el titular es parte;
  - f. El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable;
  - g. El tratamiento es necesario para tutelar intereses vitales del titular o de otra persona;
  - h. El tratamiento es necesario por asuntos de interés público previstos en la ley;
  - i. El tratamiento es necesario para satisfacer intereses legítimos perseguidos por el responsable o por un tercero, siempre que dichos intereses no prevalezcan

los intereses o derechos fundamentales del titular, con especial protección en niños, niñas y adolescentes.

2. Condiciones para el consentimiento. – La carga de demostrar el consentimiento indubitable del titular le corresponde al responsable, a través de una declaración o una acción afirmativa clara. Además, el titular puede revocar el consentimiento en cualquier momento, para lo cual el responsable debe prever mecanismos sencillos, ágiles, eficaces y gratuitos.
3. Consentimiento para el tratamiento de datos personales de niñas, niños y adolescentes. – El consentimiento en el caso de niñas, niños y adolescentes es concedido a través del titular de la patria potestad o tutela, conforme a las reglas de representación previstas en la normativa interna de cada estado. Así también, el responsable debe realizar esfuerzos razonables para verificar que el consentimiento fue efectivamente otorgado por el titular de la patria potestad o tutela.
4. Principio de licitud. – El tratamiento de datos personales debe ser realizado en estricto apego al derecho interno, el derecho internacional y los derechos y libertades fundamentales de las personas. Cuando el tratamiento sea realizado por autoridades públicas, estas deben sujetarse estrictamente a las facultades o atribuciones establecidas en la Ley y los principios aplicables a responsables privados.
5. Principio de lealtad. – La protección de los intereses del titular deben prevalecer en el tratamiento de los datos personales, absteniéndose del uso de medios engañosos o fraudulentos. Será considerado desleal el tratamiento de datos personales que den lugar a discriminaciones injustas o arbitrarias contra los titulares.
6. Principio de transparencia. – El responsable debe informar al titular sobre la existencia y la naturaleza del tratamiento al que serán sometidos sus datos personales con la finalidad de que el titular tome decisiones informadas. El responsable debe, como mínimo, proporcionar la siguiente información:
  - a. Identidad y datos de contacto.
  - b. Finalidad del tratamiento a que serán sometidos sus datos personales.
  - c. Las comunicaciones nacionales o internacionales de datos personales que se pretendan realizar, esto incluye a sus destinatarios y la finalidad por las que se realizan dichas comunicaciones.
  - d. Los mecanismos por los que el titular puede ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad.
  - e. El origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular.

7. Principio de proporcionalidad. – El responsable debe limitarse a tratar datos personales apegado al mínimo necesario, de tal manera que los datos personales que trate resulten adecuados, pertinentes y limitados.
8. Principio de calidad. – El responsable debe tomar medidas para mantener los datos personales exactos, actualizados y completos para no alterar su veracidad y en cumplimiento con las finalidades que motivan su tratamiento. Cuando estos datos hubieren dejado de ser necesarios o su tratamiento haya cumplido su propósito, el responsable debe suprimirlos o eliminarlos de sus archivos, registros, bases de datos o sistemas de información o bien someterlos a un proceso de anonimización. En el proceso de eliminación de los datos el responsable debe garantizar que sea definitiva y segura. Al cumplimiento del propósito se puede excepcionar la eliminación de los datos en casos que justifiquen su tratamiento y que estén relacionados con las obligaciones legales del responsable, siempre que estas respeten plenamente los derechos del titular.
9. Principio de responsabilidad. – Este principio consiste en la implementación de mecanismos de acreditación establecidos en estos Estándares y la rendición de cuentas al titular y a la autoridad competente sobre el tratamiento de los datos personales. El responsable puede valerse de estándares, mejores prácticas nacionales e internacionales, sistemas de autorregulación, o cualquier mecanismo que permita la consecución de este propósito. Estos mecanismos pueden incluir instrumentación de programas y políticas de protección de datos personales, sistemas de administración de riesgos, programas de capacitación y actualización, revisión periódica de políticas, etc.
10. Principio de seguridad. – Se refiere a la toma de medidas administrativas, físicas y técnicas necesarias para garantizar la confidencialidad, integridad y disponibilidad de los datos personales en consideración con los siguientes factores:
  - a. El riesgo que corren los datos en posesión de una tercera persona no autorizada para su tratamiento.
  - b. El estado de la técnica.
  - c. Los costos de aplicación.
  - d. La naturaleza de los datos.
  - e. Alcance, contexto y finalidad del tratamiento.
  - f. La transferencia internacional de datos personales.
  - g. El número de titulares.

- h. Las potenciales consecuencias de una posible vulneración para los titulares.
  - i. Las vulneraciones previas ocurridas en el tratamiento de datos personales.
11. Notificación de vulneraciones a la seguridad de los datos personales. – El responsable tiene la obligación de comunicar a la autoridad competente y al titular afectado cuando este tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento. Esto comprende cualquier daño, pérdida, alteración, destrucción, acceso no autorizado o uso ilícito de los datos personales, aún si es accidental. Esta notificación debe realizarse sin dilaciones, con un lenguaje claro y sencillo y que indique la naturaleza del incidente, los datos personales que han sido comprometidos, las acciones correctivas que han sido tomadas de forma inmediata, las recomendaciones al titular sobre las medidas que éste puede tomar para tutelar sus intereses y los medios que el titular tiene para obtener mayor información al respecto. Adicionalmente, el responsable debe documentar toda vulneración de seguridad que se dé a los datos personales en cualquier de forma pormenorizada, y detallando los hechos relacionados con ella, los efectos resultantes, las medidas correctivas tomadas inmediata y definitivamente.

Principio de confidencialidad. – Por este principio, el responsable debe establecer mecanismos para que todos los agentes que intervienen en el tratamiento de datos personales respeten la confidencialidad de los mismos, sea cual fuere la fase del tratamiento de datos personales e incluso en lo posterior a la culminación de su relación con el titular. (Red Iberoamericana de Protección de Datos, 2017)

Luego de identificar todos estos principios que han sido desarrollados en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, se puede evidenciar que los criterios tomados por la RIPD son innovadores y establecen una serie de mínimos que responden al propósito de la protección de datos personales; pues, a través de éstos, los estados tienen lineamientos efectivos para desarrollar una adecuada y estandarizada reglamentación sobre este derecho fundamental. Aquellos no han pasado desapercibidos a los ojos del legislador ecuatoriano, pues sirvieron de inspiración y como motivación para la promulgación de la Ley Orgánica de Protección de Datos Personales que es materia de análisis de la presente investigación. Resulta claro a este punto, que el rol de los organismos multilaterales de integración como la ONU y la RIPD han propiciado el criterio de la Asamblea Nacional al momento de formular la legislación interna de Ecuador como se evidencia en los “considerando” que el pleno tuvo para expedir esta norma. (Ley Orgánica de Protección de Datos Personales, 2021)

### 2.3. Marco Constitucional del derecho a la protección de datos personales.

La actual Constitución de la República del Ecuador o Constitución de Montecristi que se encuentra vigente desde 2008 se vincula al derecho a la protección de datos primordialmente a través de dos derechos constitucionales que amparan esta institución. El primero es a través del derecho a la protección de datos de carácter personal que está reconocido en el artículo 66 numeral 19, cuyo texto establece lo siguiente:

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

(...) 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. (Constitución de la República del Ecuador, 2008)

Como se puede evidenciar, el derecho a la protección de datos de carácter personal alcanza el rango de derecho fundamental, consagrado específicamente en la norma suprema del Ecuador. En la historia constitucional de la República, la actual Constitución es el primer instrumento de esta naturaleza que reconoce expresamente el derecho a la protección de datos como parte del catálogo de derechos de las personas. Como se demostró con antelación, las constituciones que antecedieron a la actual amparaban al derecho a la protección de datos como un derecho accesorio que surge a consecuencia del derecho a la privacidad y del derecho a la intimidad, a su vez también como resultado de la rectificación y acceso a la información que permitía en su momento la garantía constitucional del habeas data tal y como se explicó con la Ley de Control Constitucional y la Constitución de 1998.

Es decir que, a pesar de los progresos tecnológicos y digitales que ya desde el Siglo XX se desarrollaban en la sociedad, no fue sino hasta el 2008 que el constituyente reconoce la imperatividad de proteger y tutelar los datos personales como una garantía fundamental de las personas. Concomitantemente, el legislador hace énfasis en el papel de la voluntad del titular para el tratamiento en todas sus formas o bien en apego a la legalidad, ergo, que el tratamiento sin el consentimiento de los titulares únicamente puede darse si se encuentra en algún supuesto recogido en la ley.

Complementariamente, el artículo 92 de la Constitución desarrolla la institución jurídica del habeas data cuyo desarrollo histórico constitucional ha sido explicado con antelación. En la actual carta magna, el habeas data nace como garantía de:

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.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

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

La acción de habeas data tal y como está plasmada en el artículo 92 responde a una serie de derechos vinculados al acceso, conocimiento, rectificación y eliminación de información personal cuya tutela es integral y comprende varios escenarios para garantizar su defensa integral y lógica. Es destacable, por ejemplo, que la acción de habeas data apara tanto a la persona titular del derecho, como a su propiedad, evitando un supuesto en el que los derechos de la persona titular sean vulnerados por que la información no sea sobre sí si no sobre su propiedad. Esta serie de derechos también contempla los dos tipos de entidades o personas responsables del custodio de la información, pudiendo ser exigibles tanto a personas jurídicas privadas como al propio Estado representado por las entidades públicas.

En conclusión, la acción de habeas data tal y como está plasmada en la Constitución de la República constituye una compleja institución jurídica que aglomera un conjunto de derechos vinculados a los datos personales, su acceso, rectificación, eliminación, restricción de difusión y la consecuencia de ser reparado por cualquier vulneración a las garantías contempladas en el habeas data.

Las acciones constitucionales tienen su desarrollo normativo en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. La acción de habeas data está reglamentada en el capítulo VI de dicha norma para lo cual el legislador ha establecido en los artículos 49, 50 y



51 el objeto de la acción de habeas data como garantía jurisdiccional, su ámbito de protección y la legitimación activa de la misma:

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.

El titular de los datos podrá solicitar al responsable del archivo o banco de datos, el acceso sin costo a la información antes referida, así como la actualización de los datos, su rectificación, eliminación o anulación. No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos.

Las personas responsables de los bancos o archivos de datos personales únicamente podrán difundir la información archivada con autorización del titular o de la ley.

Las presentes disposiciones son aplicables a los casos de rectificación a que están obligados los medios de comunicación, de conformidad con la Constitución.

El concepto de reparación integral incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación. (Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009)

No mucho varía con respecto al objeto descrito en el artículo 92 de la Constitución de la República; sin embargo, se observa que la LOGJCC sí prevé precisiones sobre la gratuidad de solicitar al responsable el acceso a su información y su actualización, rectificación, eliminación o anulación; y la imposibilidad de solicitar la eliminación de información que por mandato legal debe ser pública. Adicionalmente, el objeto precisa lo que se analizó en los principios previstos por la RIPD y la Asamblea General de la ONU sobre la legalidad del intercambio de información, aquel consentimiento previo del titular o bien la autorización legal para poder difundir la información archivada.

En virtud del artículo 50, el ámbito de protección es procedente en los siguientes supuestos:



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. (Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009)

Finalmente, es necesario precisar que la acción de habeas data puede ser interpuesta por toda persona natural o jurídica, por sus propios derechos o como representante legitimado para el efecto, esto en virtud del artículo 51 de la LOGJCC. (Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2009)

### **Capítulo III**

#### **Análisis comparativo entre los Principios Actualizados sobre Privacidad y la Protección de Datos Personales del Comité Jurídico Interamericano de la Organización de Estados Americanos y la Ley Orgánica de Protección de Datos Personales del Ecuador.**

##### **3.1. Análisis del listado de Principios Actualizados sobre la Privacidad y la Protección de Datos Personales de la OEA.**

Los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales son una serie de lineamientos que fueron aprobados en la Organización de Estados Americanos el 11 de noviembre de 2021 a través de la Resolución AG/RES. 2974 (LI-O/21). Estos principios, tal y como su nombre lo describe, son una actualización a los estándares que fueron adoptados en 2012 por el Comité Jurídico Interamericano; pues, en observancia de la necesidad de actualizar dichos lineamientos en razón de su fortalecimiento, revisión y adaptación a la evolución tecnológica y normativa del tratamiento y protección de datos personales.

Este fue un proceso que involucró a varios actores y organizaciones internacionales que brindaron valiosos aportes en la consecución de estos principios, entre ellos, la ya analizada

Red Iberoamericana de Protección de Datos, junto con una relatoría especial para la tarea en cuestión y sujetándose a un gran proceso de consultas tanto a estas organizaciones como a Estados Miembros de la Organización.

En palabras de Dante Negro (2021), se trata de un instrumento de soft law que, a pesar de no ser un instrumento vinculante para los estados miembros de la OEA, son un referente para el fortalecimiento de sus marcos jurídicos en materia de privacidad y protección de datos y guiar el desarrollo colectivo de la región hacia una protección armónica y efectiva de los datos personales. (Organización de Estados Americanos, 2022)

Estos principios fueron desarrollados por el Comité Jurídico Interamericano, que es un órgano constitutivo de la Organización de Estados Americanos y que, en virtud del artículo 99 de la Carta de la Organización, sirve como cuerpo consultivo en asuntos jurídicos, promueve el desarrollo progresivo y la codificación del derecho internacional, y estudia los problemas jurídicos de la integración de los países en desarrollo del Continente y la posibilidad de uniformar sus legislaciones en cuanto parezca conveniente. (Carta de la Organización de Estados Americanos, 1948)

Se hace énfasis en esta última función que tiene el Comité Jurídico Interamericano (en adelante también CJI), como se pudo evidenciar anteriormente, el flujo transfronterizo de datos ha creado esta necesidad de armonizar las regulaciones en materia de protección de datos personales, y es precisamente lo que estos principios materializan al servir de guía a los estados miembros para la regulación paulatina, coherente y sintonizada de los datos personales.

### **3.1.1. Principio Uno. – Finalidades Legítimas y Lealtad.**

Los datos personales deberían ser recopilados solamente para finalidades legítimas y por medios leales y legítimos. (Organización de Estados Americanos, 2022)

Este principio enfoca su utilidad en la legitimidad en dos aristas. La primera está vinculada al propósito de la recopilación de datos y se refiere a la obtención consentida e informada por parte del titular de los datos. Es decir, que el titular debe estar informado de cuál es la finalidad o la necesidad de otorgar sus datos al responsable, que el tratamiento sea necesario para cumplir una obligación legal aplicable al responsable, que el tratamiento sea imperativo por asuntos de interés público o que el tratamiento responda una orden de autoridad judicial.

La segunda arista alude al medio a través del cual se recopilan los datos. Esto implica una abstención de recurrir a la obtención de datos a través de conductas y medios ilícitos,

fraudulentos o incurrir al engaño. A su vez, implica un mandato al responsable de ser transparente e informar al titular el uso y destino de los datos, al momento de recopilarlos.

Como se puede observar, este principio guarda estrecha similitud con el principio de legitimación de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de la RIPD, con la diferencia notable que la segunda desarrolla con mayor especificidad y amplitud los escenarios en los que la legitimación se configura.

### **3.1.2. Principio Dos. – Transparencia y consentimiento.**

Antes o en el momento en que se recopilen, se deberían especificar la identidad y datos de contacto del responsable de los datos, las finalidades específicas para las cuales se tratarán los datos personales, el fundamento jurídico que legitima su tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida y los derechos del titular en relación con los datos personales a ser recopilados. Cuando el tratamiento se base en el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento previo, inequívoco, libre e informado de la persona a que se refieran. (Organización de Estados Americanos, 2022)

Este principio, al igual que el anterior, está conformado por dos aspectos que deben ser abordados separada y conjuntamente para entender sus particularidades y también el porqué de su unión para devenir un principio único para el CJI. En un primer plano, la transparencia alude primordialmente a la capacidad del titular de poder identificar aspectos relacionados a sus datos, su uso y la finalidad de su tratamiento. En CJI ha considerado que la transparencia debe ser una característica palpable al momento de recopilar los datos. En este momento, el titular debe ser capaz de poder identificar al responsable del tratamiento, cuál es la finalidad del tratamiento, el fundamento jurídico o la base legal mediante la cual se recopilan y tratan los datos, todos los destinatarios de los datos y los mecanismos que tiene para poder ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad.

Es a través de esta transparencia que el titular es capaz de tomar decisiones informadas y fundamentadas en las circunstancias reales y actuales por las que da su consentimiento para que sus datos personales sean tratados o manejados por el responsable o por delegados que puedan involucrarse en el proceso de tratamiento de datos. Sin esta transparencia, el consentimiento del titular estaría viciado y no sería válido propiamente.

Por otra parte, el consentimiento se refiere precisamente a la manifestación de voluntad libre de vicios del titular de los datos personales. Este consentimiento es el resultado de un proceso

de legitimación que surge a partir de la dotación de información necesaria para tomar una decisión válida y fundamentada. Es decir, que el consentimiento en materia de protección de datos es el resultado de la proporción de información transparente, sencilla y entendible al titular, de tal manera que aquel resulte en una manifestación legítima de voluntad.

Como es evidente, la transparencia evita que el titular corra riesgos al momento de consentir el tratamiento de sus datos, evitando que éste sea víctima de engaño, intimidación, coacción o consecuencias inesperadas del tratamiento de sus datos o a su vez, de no dar consentimiento a su tratamiento. El principio de transparencia constituye entonces una obligación para el responsable de suministrar información relativa al tratamiento de datos, antes del tratamiento en aras de validar el consentimiento del titular y durante el tratamiento a través del derecho de acceso, rectificación y actualización en caso que la finalidad del tratamiento ha cambiado a la última que el titular haya dado su consentimiento.

### **3.1.3. Principio tres. – Pertinencia y Necesidad.**

Los datos personales deberían ser únicamente los que resulten adecuados, pertinentes y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior. (Organización de Estados Americanos, 2022)

La pertinencia se basa en una relación razonable entre los datos que han sido recopilados para tratamiento y la finalidad del tratamiento. Es decir que, el tratamiento de los datos personales debe cumplir un propósito que justifica razonablemente su manejo. La necesidad tiene estrecha similitud con la pertinencia en razón de que el tratamiento de los datos personales debe estar justificado por la finalidad perseguida, sin embargo, la necesidad responde a un criterio de minimización o limitación en el tratamiento de dichos datos, esto se traduce a un estándar de datos que sean pertinentes y que se rijan al mínimo de intrusión posible.

### **3.1.4. Principio cuatro. – Tratamiento y conservación limitados.**

Los datos personales deberían ser tratados y conservados solamente de manera legítima no incompatible con las finalidades para las cuales se recopilaron. Su conservación no debería exceder del tiempo necesario para cumplir dichas finalidades, de conformidad con la legislación nacional correspondiente. (Organización de Estados Americanos, 2022)

Este principio se fundamenta en dos aspectos. En primer lugar, existe el tratamiento limitado de datos que hace referencia al manejo prolijo, legítimo y apegado a los motivos que llevaron

al titular a dar su consentimiento. El principio cuatro alude a esta compatibilidad que debe existir entre el tratamiento y la finalidad de recopilación, es decir, que el conocimiento y consentimiento del titular van a ser el campo de acción en el cual el responsable puede maniobrar en el tratamiento de datos. El límite que encuentra el responsable en cuanto al tratamiento debe ser aquel al que el titular, en ejercicio de su autodeterminación ha impuesto, con la única excepción siendo los supuestos que estén establecidos en la Ley.

Este principio a su vez se fundamenta en la conservación limitada. Como se ha analizado anteriormente, los datos personales reúnen información que precisamente por su naturaleza permiten ser atribuidos a una persona e identificar a su titular con facilidad. Esto es una herramienta que puede tornarse atentatorio y posicionar al titular en una situación de vulnerabilidad en cuanto la conservación de datos durante o después de su tratamiento no ha sido limitada. En este sentido, este principio prevé que la conservación de los datos también se regule razón de que la sola conservación de datos acarrea sus riesgos. La conservación puede ser limitada a través de dos formas: La eliminación de los datos o su anonimización.

### **3.1.5. Principio cinco. – Confidencialidad.**

Los datos personales no deberían divulgarse, ponerse a disposición de terceros, ni emplearse para otras finalidades que no sean aquellas para las cuales se recopilaron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley. (Organización de Estados Americanos, 2022)

En el análisis del propio CJJ, la confidencialidad es un deber básico que tiene el responsable ante el tratamiento de datos personales en un entorno seguro y controlado. Este principio es el mandato de no divulgar y que su divulgación solo esté permitida en la medida en que el consentimiento del titular lo permita y bajo los supuestos legales correspondientes.

### **3.1.6. Principio seis. – Seguridad de los Datos.**

La confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas, administrativas u organizacionales razonables y adecuadas contra tratamientos no autorizados o ilegítimos, incluyendo el acceso, la pérdida, destrucción, daños o divulgación, aún cuando éstos ocurran de manera accidental. Dichas salvaguardias deberían ser objeto de auditoría y actualización permanente. (Organización de Estados Americanos, 2022)

Este principio contiene un mandato para el responsable, que consiste en la adopción de salvaguardias (mecanismos) de seguridad de diversa índole con la finalidad de garantizar, en la medida de lo razonable y posible, que los datos se encuentran a buen recaudo. Este mandato incluye no solamente el resguardo pasivo de los datos personales, si no que las salvaguardias deben ser más rigurosas en razón de la naturaleza de los datos. Mientras más sensibles son los datos en custodia del responsable, mayores deben ser las medidas de seguridad aplicadas a su resguardo.

Sin embargo, algo que se reconoce desde la Organización de Estados Americanos es que, en la actualidad resulta casi imposible garantizar un sistema invulnerable a un ataque o vulneración externa. Actualmente la mayoría de ficheros y bases de datos que contienen datos personales reposan en soportes electrónicos o digitales, lo que implica siempre que pueden existir atentados cibernéticos a estas bases y la información corre riesgo. Es por ello, que este principio no es un mandato a establecer barreras inquebrantables, si no a que dichas salvaguardias respondan los mejores criterios de seguridad en cuanto al resguardo de la información, sea cual fuere la naturaleza de los soportes en los que reposan los datos personales.

Paralelamente, la OEA destaca que, por lo general, la normativa en materia de protección de datos personales usualmente requiere que, en caso de ataques o vulneraciones a la seguridad de los datos personales, el responsable suele estar obligado a notificar dichos sucesos a los titulares y a las autoridades de control. Esto permite realizar evaluaciones a las salvaguardias de los responsables y a su vez evitar la impunidad de actos tipificados como infracciones penales para su respectiva investigación.

### **3.1.7. Principio siete. – Exactitud de los Datos.**

Los datos personales deberían mantenerse exactos, completos, y actualizados hasta donde sea necesario para las finalidades de su tratamiento, de tal manera que no se altere su veracidad. (Organización de Estados Americanos, 2022)

La exactitud de los datos deviene un mandato al responsable de datos de mantener actualizados, exactos, completos y accesibles a cualquier corrección o modificación por parte del titular. A través de este principio, lo que se pretende es que el mantenimiento y la conservación de datos sea un deber de actualización continua por parte del titular, a su vez, y en cumplimiento de los principios tres y cuatro, el responsable debe mantener los datos actualizados durante el tiempo que cumplen con la finalidad por los que fueron recopilados y tratados. Una vez esta finalidad ha sido cumplida, la exactitud de los datos implicaría que los mismos sean eliminados.

### **3.1.8. Principio ocho. – Acceso, Rectificación, Cancelación, Oposición y Portabilidad.**

Se debería disponer de métodos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados, puedan solicitar el acceso, rectificación y cancelación de los mismos, así como el derecho a oponerse a su tratamiento y, en lo aplicable, el derecho a la portabilidad de esos datos personales. Como regla general, el ejercicio de esos derechos debería ser gratuito. En caso de que fuera necesario restringir los alcances de estos derechos, las bases específicas de cualquier restricción deberían especificarse en la legislación nacional y estar en conformidad con los estándares internacionales aplicables. (Organización de Estados Americanos, 2022)

Es notorio que este principio en realidad cumple mayoritariamente con la función de establecer una serie de derechos básicos para los titulares de datos. En el principio anterior, se determinó que la exactitud de los datos personales es una obligación que a la par le corresponde al responsable o al encargado de datos. Sin embargo, la exigibilidad de la exactitud también debe constituir un derecho que le corresponde al titular.

Dicho esto, el derecho a recurrir estos datos, impugnar su exactitud y pedir al responsable su revisión, modificación, corrección o eliminación es un derecho perenne y fundamental de los titulares. EL CJI reconoce que aquello representa una de las salvaguardias más importantes en el campo de la protección de datos y la privacidad (Organización de Estados Americanos, 2022).

La OEA establece que los elementos esenciales de este principio son:

1. La capacidad de la persona para obtener Datos relacionados con ella en un plazo razonable y de una forma razonable e inteligible, para saber si se ha denegado una solicitud de acceso a dichos datos y por qué;
2. La capacidad de impugnar tal denegación.

El habeas data como acción y derecho que le corresponde al titular es el cimiento sobre el que se fundamenta este principio, como un mecanismo jurídico mediante el cual el titular puede eficazmente tener acceso a su información en posesión de terceros, su rectificación y

su eliminación. Tanto así que varios ordenamientos jurídicos a nivel interamericano cuentan con la acción (o derecho, en los casos que así corresponde) de habeas data aún si no cuentan con una Ley específica en materia de protección de datos personales.

En el caso ecuatoriano, como fue analizado con antelación el habeas data tiene tal prevalencia en nuestro sistema jurídico-normativo que éste constituye una acción constitucional que encuentra su regulación mucho antes que la promulgación de la Ley Orgánica de Protección de Datos Personales, siendo este un mecanismo jurisdiccional para hacer valer los derechos vinculados a este principio.

Sin embargo, este principio no tiene porqué limitarse al establecimiento de mecanismos jurisdiccionales para hacer valer tales derechos. Es decir que, estos derechos no requieren activar el aparataje jurisdiccional del Estado y hacer valer estos derechos a través de la judicialización de un caso en específico. En todo caso, esta serie de derechos han devenido algo simple, automático y de ejercicio inmediato. En consecuencia, no es necesario tener que demandar y convocar a un juez para que vele por los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

En los casos en los que este acceso inmediato sea negado a los titulares, deben existir mecanismos para revisar e impugnar tal denegación. Estos mecanismos permitirán que la revisión de la denegación sea efectuada en Derecho, en el sentido en que tal denegación no puede ser arbitraria, si no que únicamente podría ser efectuada en las causas establecidas en la Ley o en la convención o contrato que llevó al titular a dar su consentimiento. Es decir, el derecho de acceso no es absoluto, sin embargo, en los casos en los que aquel encuentre límites, estos deben ser legales o convencionales y no pueden ser unilaterales ni arbitrarios. En todo caso, el titular debe contar siempre con la facultad de poder recurrir o impugnar tal denegación.

Paralelamente, la persona debe contar con mecanismos inmediatos para ejercer el derecho de rectificación con la finalidad de corregir, precisar o actualizar sus datos. En virtud del principio siete, la exactitud de los datos es a su vez un deber del responsable o del encargado, pero a su vez, existe la obligación de estos últimos de rectificar o corregir los datos cuando el titular lo solicite bajo las condiciones que la Ley establezca y siempre que estas modificaciones persigan precisamente la exactitud de los datos y no estén encaminadas a inducir al engaño o al fraude.

El Derecho a la cancelación se refiere a la capacidad del titular de retirar su consentimiento u oponerse a su tratamiento en razón de los requerimientos, plazos términos y condiciones



en las que los titulares pueden ejercerlo. A su vez, el derecho de oposición se refiere, como su nombre lo dice, a la capacidad del titular de oponerse al tratamiento de sus datos personales en función de una razón legítima o cuando tenga por objeto la elaboración de perfiles para mercadotecnia directa.

Finalmente, el derecho a la portabilidad de los Datos Personales consiste en la capacidad del titular de determinar la transferencia de los mismos entre responsables. Esta transferencia debe ser técnicamente posible y no debe ser de información derivada que haya sido resultado del tratamiento de dichos datos y cuya titularidad le corresponda al responsable y no al titular de datos.

#### **3.1.9. Principio nueve. – Datos Personales sensibles.**

Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos. (Organización de Estados Americanos, 2022)

El CJI precisa que el término “Datos Personales Sensibles” son los que más se vinculan con la intimidad de sus titulares. La razón de su especial protección se fundamenta en el riesgo de intromisión profunda en la dignidad personal, el honor y libertades fundamentales del titular en caso de ser divulgados o que sus salvaguardias sean burladas. Consecuentemente, este principio manda a que los estados establezcan categorías especiales de datos personales que sean especialmente sensibles. A través de esta categorización de datos personales se pueden establecer estándares normativos mínimos pertinentes y el alcance de la prohibición del Tratamiento de Datos Personales sensibles o el establecimiento de condiciones especiales y específicas para su tratamiento.

#### **3.1.10. Principio diez. – Responsabilidad.**

Los responsables y encargados del tratamiento de datos deberían adoptar e implementar las medidas técnicas y organizacionales que sean apropiadas y efectivas para asegurar y poder demostrar que el tratamiento se realiza en conformidad con estos Principios. Dichas medidas deberían ser auditadas y actualizadas periódicamente. El responsable o encargado del tratamiento y, en lo aplicable, sus representantes, deberían cooperar, a petición, con las autoridades de protección de

datos personales en el ejercicio de sus tareas. (Organización de Estados Americanos, 2022)

Mucho se alude a los términos responsable y responsabilidad en materia de protección de datos. A esta noción de la responsabilidad como un principio rector en la materia se la considera esencial para asegurar la implementación efectiva de un marco de protección de datos. Esta responsabilidad requiere que los gestores de datos, conocidos como responsables cumplan con todos los principios paralelos a la responsabilidad y demostrar este cumplimiento a través de indicadores medibles. (United Nations Development Programme, 2023)

En los términos en los que el CJI ha planteado a la responsabilidad como principio, esta debe ser entendida como el mandato a los Responsables de Datos de implementar medidas organizacionales y técnicas necesarias para asegurar que el Tratamiento de datos se cumple en los términos y lineamientos de los principios y, a su vez, con la normativa aplicable a la materia. A los criterios del Programa de las Naciones Unidas para el Desarrollo, el CJI se suscribe en reconocer que el enfoque idóneo para el cumplimiento de un sistema eficiente de protección de datos, el diseño de sistemas y la arquitectura de la tecnología utilizada para el tratamiento, recopilación y manejo en general de datos personales deben consolidarse con la “privacidad como diseño”. Este concepto, es una forma de responsabilidad proactiva que consiste en considerar los riesgos potenciales en función de la naturaleza de los datos recopilados y/o tratados. A criterio del PNUD este concepto tiene tal relevancia que forma parte de uno de los siete criterios que toma en cuenta el programa para operativizar la transparencia y la responsabilidad en los procesos de tratamiento de datos personales, siendo estos siete los siguientes:

1. La adopción de la privacidad como diseño,
2. Proveer acceso a los titulares a su información,
3. Adopción de salvaguardias en materia de seguridad,
4. Reportar los casos de ataques a las salvaguardias de seguridad,
5. Llevar registros del tratamiento de datos personales,
6. Realizar evaluaciones de impacto sobre protección de datos, como una herramienta que permite de manera anticipada analizar los riesgos a los que los datos personales están expuestos en función de las actividades de tratamiento (DPIA por sus siglas en inglés).
7. Designación de encargados de monitorear la protección de datos. (United Nations Development Programme, 2023)

**3.1.11. Principio once. – Flujo transfronterizo de Datos y Responsabilidad.**

Reconociendo su valor para el desarrollo económico y social, los Estados Miembros deberían cooperar entre sí para facilitar el flujo transfronterizo de datos personales a otros Estados cuando éstos confieran un nivel adecuado de protección de los datos de conformidad con estos Principios. Asimismo, los Estados Miembros deberían cooperar en la creación de mecanismos y procedimientos que aseguren que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción, o los transmitan a una jurisdicción distinta de la suya, puedan garantizar y ser efectivamente hechos responsables por el cumplimiento de estos Principios. (Organización de Estados Americanos, 2022)

Una de las consideraciones más relevantes que llevó al Comité Jurídico Interamericano a considerar el establecimiento de los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales fue precisamente el reconocimiento del fenómeno del flujo transfronterizo de datos y las necesidades de integración jurídica que los Estados Miembros de la Organización de Estados Americanos en la materia. En este sentido, la cooperación internacional resulta imperativa en el desarrollo económico y social de las naciones.

A pesar del notorio crecimiento de flujo transfronterizo de bienes, servicios e información, no existe estandarización en materia de protección de datos personales en las diversas jurisdicciones en las que se desarrolla dicho flujo. El CJI reconoce que esta incompatibilidad jurídica puede generar confusión, conflicto y contradicciones, de ahí que nace la necesidad de estandarizar la reglamentación entre los países en los que el flujo transfronterizo de datos es un hecho.

A través de los mecanismos de cooperación internacional la balanza debe tornarse a favor de la integración y la supresión de conflictos entre enfoques jurídicos que rigen el uso y transferencia de datos personales (Organización de Estados Americanos, 2022). Uno de los riesgos que corren los datos personales y, consecuentemente, los derechos de sus titulares es precisamente la precariedad legal en la que se pueden encontrar al momento de cruzar de una frontera a otra, figurativamente hablando. Sin ninguna intención de desmerecer los sistemas jurídicos de un país, puede suscitarse que la protección o las condiciones por las que los titulares otorgaron el consentimiento para su tratamiento, o los estándares de salvaguardias a los sistemas en los que reposan los datos pueden ser menos rigurosos en un Estado que en otro. Como consecuencia y jurídicamente hablando, la incompatibilidad de

reglamentación inter Estados podría acarrear vicios irreparables al fundamento más esencial del tratamiento de datos personales que es precisamente el consentimiento de los titulares.

Una solución parcial que al menos cubre el dilema de cómo responsabilizar a los responsables o qué fuero jurisdiccional aplicar a quien está encargado del tratamiento de datos personales es precisamente el de responsabilizarlo en razón de su domicilio social y que la protección de datos personales esté garantizada bajo los estándares a los que el responsable se somete aun cuando la información objeto de protección se encuentre fuera de tal frontera.

Finalmente, el CJI reconoce, al igual que como posteriormente se evidenció con la Red Iberoamericana de Protección de Datos y la Organización de las Naciones Unidas, que el establecimiento de principios de protección de datos personales a través de organismos intergubernamentales responde al objetivo de estandarizar entre sus Estados Miembro las reglas de protección de datos.

#### **3.1.12. Principio doce. – Excepciones.**

Cualquier excepción a alguno de estos Principios debería estar prevista de manera expresa y específica en la legislación nacional, ser puesta en conocimiento del público y limitarse únicamente a motivos relacionados con la soberanía nacional, la seguridad nacional, la seguridad pública, la protección de la salud pública, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público o el interés público. (Organización de Estados Americanos, 2022)

Evidentemente la protección de datos y la privacidad no son los únicos derechos e intereses que un Estado debe tutelar y; consecuentemente, no pueden ser elementos absolutos ni inamovibles en un Estado de Derecho. En este sentido, la privacidad y la protección de datos personales deben encontrar límites en cuanto estos son necesarios para tutelar y salvaguardar bienes jurídicos del resto de ciudadanos y de la sociedad misma.

Las excepciones a la protección de datos personales deben imperativa y puntualmente estar recogidas en el ordenamiento jurídico de los Estados y no pueden jamás ser, aunque suene redundante, la regla. Por medio de normas públicas los Estados deben taxativamente enumerar las excepciones a la protección de datos personales, los casos concretos y los supuestos en los que tales protecciones no aplican, respondiendo a un interés ulterior como los enlistados en este principio.

### **3.1.13. Principio trece. – Autoridades de Protección de Datos.**

Los Estados Miembros deberían establecer órganos de supervisión independientes, dotados de recursos suficientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos personales de conformidad con estos Principios. Los Estados Miembros deberían promover la cooperación entre tales órganos. (Organización de Estados Americanos, 2022)

Algo que destacar en este principio es el mandato a establecer órganos independientes. Esta característica de la Autoridad de Protección de Datos toma mucha relevancia cuando se considera que no únicamente personas y sociedades privadas son las que se encargan de tratar o recopilar datos personales, si no que estos pueden estar en posesión de entidades gubernamentales, entidades o empresas públicas y que obviamente no están exentas del control y cumplimiento de las regulaciones en la materia; consecuentemente, es de vital importancia que la independencia de los organismos de control sea garantizada para evitar arbitrariedad, corrupción o abuso de poder de parte de entidades públicas en el control del cumplimiento de estos estándares.

### **3.2. Análisis del listado de principios establecidos en la Ley Orgánica de Protección de Datos Personales.**

La Ley Orgánica de Protección de Datos Personales nace como iniciativa del ejecutivo en el año 2019 como consecuencia de la filtración de datos más grande que haya tenido Ecuador hasta la fecha. El presidente en turno, el licenciado Lenín Moreno Garcés propuso ante la Asamblea Nacional la promulgación de una ley que regulase específicamente el derecho a la protección de datos personales.

La Ley Orgánica de Protección de Datos Personales (en adelante LOPDP) fue el resultado del trabajo de la entonces directora de la Dirección Nacional de Registro de Datos Públicos (DINARDAP) quien, junto con otras instituciones privadas y públicas y la participación de la sociedad civil se consolida una iniciativa legislativa que permita el desarrollo de la innovación y el uso de la tecnología teniendo como enfoque central el tratamiento de los datos personales. (Cabezas Mena & Lucas Franco, 2023)

Como ha sido objeto previo de análisis, las motivaciones jurídicas y constitucionales de poder garantizar el derecho a la protección de datos de carácter personal, a más de los instrumentos internacionales que han sido promulgados en la materia a nivel de la Organización de las Naciones Unidas, la Red Iberoamericana de Datos Personales y la Organización de Estados Americanos, fue precisamente el reconocimiento de este derecho como parte del repertorio de derechos constitucionales recogidos en el artículo 66, más precisamente en su numeral 19; por lo que solo era cuestión de iniciativa que Ecuador empiece a regular oportunamente los principios, reglas y procedimientos por los que se haría efectivo tal derecho.

La LOPDP fue publicada en el Quinto Suplemento N.º 459 del Registro Oficial el 21 de mayo de 2021, esta fue sometida a dos debates en el Pleno de la Asamblea Nacional, el primero los días 9 y 11 de febrero de 2021 y el segundo el 10 de mayo de 2021. Entre los aspectos considerados por el Pleno para aprobar esta norma también tomó en cuenta el Programa de Gobierno Abierto del Plan Nacional de Gobierno Electrónico que apuntaba a “impulsar la protección de la información y datos personales”. (Ley Orgánica de Protección de Datos Personales, 2021)

En el artículo 10 de la Ley Orgánica de Protección de Datos Personales se establecen los principios por los cuales se rige dicho cuerpo normativo, sin perjuicio de los demás principios establecidos en los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, son un total de trece principios que serán objeto de análisis en el siguiente apartado:

### **3.2.1. Principio de juridicidad. –**

Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los Instrumentos internacionales, la presente Ley, su Reglamento y la demás normativa y jurisprudencia aplicable. (Ley Orgánica de Protección de Datos Personales, 2021)

El principio de juridicidad es una garantía normativa en la LOPDP de que el tratamiento de los datos personales será apegado a derecho y dota de seguridad jurídica a todos los sujetos involucrados en tal proceso. La juridicidad tal y como está planteada en el artículo 10 literal a de esta Ley no solo garantiza el cumplimiento de la misma, si no que siguiendo el modelo ejemplo de la cláusula abierta de aplicación de principios, derechos y obligaciones que estén contenidas incluso en instrumentos internacionales ratificados por Ecuador. Adicionalmente, hay que tener en cuenta que los datos personales en general son un asunto multidisciplinario que requiere, a más de una normativa de regulación específica, que todo el ordenamiento

jurídico se interrelacione para dar eficaz vigencia a los derechos que se pretenden amparar, por lo que este principio prevé que al tratamiento de datos se le apliquen las demás normas del ordenamiento jurídico que le sean aplicables y no es una ley restrictiva en cuanto hace que la misma sea excluyente en cuanto a la aplicación de otras disposiciones normativas. (Caldas, 2022)

### 3.2.2. Principio de lealtad. –

El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados.

En ningún caso los datos personales podrán ser tratados a través de medios o para fines ilícitos o desleales. (Ley Orgánica de Protección de Datos Personales, 2021)

El Principio de Lealtad no es un término nuevo en la presente investigación. Es un principio que fue introducido por la Organización de las Naciones Unidas y que ha sido explicado con antelación tanto en el contexto Iberoamericano como en el del CJI de la Organización de Estados Americanos. En el caso de la LOPDP se puede evidenciar un desarrollo mucho más prolijo en cuanto a la relación entre el titular y su conciencia y conocimiento en cuanto al tratamiento de sus datos personales. Queda claro que, para no quebrantar el principio de lealtad, la licitud es un requisito básico. El principio de lealtad ha sido considerado en los tres niveles internacionales que han sido objeto de estudio en la presente investigación; la resolución 45/95 enfoca su principio de lealtad en no desviar el tratamiento de datos personales a objetivos que sean incompatibles con los principios de la Carta de las Naciones Unidas, la RIPD ha tomado en cuenta en sus estándares que la lealtad considera la prevalencia de los intereses del titular y la abstención de recurrir a medios fraudulentos de obtención de datos. Finalmente, en los Principios Actualizados sobre la Privacidad y la Protección de Datos de la OEA, prima el criterio de los medios leales, es decir los métodos a través de los cuales el responsable recopila los datos personales y que estos sean obtenidos consentida e informadamente.

Entre estos criterios se evidencia que el denominador común es la abstención de conductas desleales y fraudulentas que socaven los principios que regulan cada nivel internacional y, en el caso de Ecuador, que los fines o los medios sean ilícitos o desleales.

### 3.2.3. Principio de Transparencia. –

El tratamiento de datos personales deberá ser transparente, por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro.

Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia. (Ley Orgánica de Protección de Datos Personales, 2021)

El principio de Transparencia en la LOPDP se centra en la capacidad del titular de comprender el tratamiento. Como se ha demostrado anteriormente, el consentimiento del titular es un requisito sine qua non para validar la recopilación y el tratamiento de datos personales; sin embargo, este consentimiento debe estar libre de todo vicio y la transparencia viabiliza que el titular sepa exactamente qué es lo que está autorizando y qué es lo que se hará con su información los límites que tiene la persona a la que entrega sus datos.

### 3.2.4. Principio de finalidad. –

Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular: no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.

El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista. (Ley Orgánica de Protección de Datos Personales, 2021)

Este principio limita el tratamiento de los datos personales en función del acto que legitima su tratamiento en primer lugar: el consentimiento. Resulta adecuado afirmar que, el principio de finalidad es retroactivo al momento de recopilación de datos personales en cuanto ésta debe



ser comunicada en términos explícitos y determinados al titular y con finalidades legítimas, resultaría inaudito que las finalidades por las que se procuran recopilar y tratar datos personales no le sean comunicadas al titular desde un inicio y, en los términos de éste literal del artículo 10, que existan causales legales para que el tratamiento pueda ser extendido o rebase los términos por los que inicialmente se otorgó el consentimiento.

Algo particular sobre el Principio de Finalidad en la LOPDP es la consideración de las “expectativas razonables” del titular en su relación con el responsable. Esta terminología no está claramente definida en el presente principio y podría evidentemente acarrear cierta arbitrariedad en cuanto a lo que se consideran las expectativas razonables, la naturaleza de los datos personales y las consecuencias del tratamiento ulterior previsto. Generalmente este tipo de mandatos que no definen bien cuáles son las excepciones a la regla principal pueden generar confusión o una interpretación errónea o contradictoria eventualmente.

### **3.2.5. Principio de pertinencia y minimización de datos personales. –**

Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento. (Ley Orgánica de Protección de Datos Personales, 2021)

Tanto en los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales, como en la LOPDP la pertinencia y la minimización se consolidan en un principio cuya función es la de intervenir en lo menos posible en la información del titular. La pertinencia se fundamenta en una relación lógica que responda el para qué de la recopilación y tratamiento de los datos personales y su respuesta simplemente debe ser la finalidad por la que el titular otorgó su consentimiento.

### **3.2.6. Principio de Proporcionalidad del tratamiento. –**

El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o a la naturaleza misma, de las categorías especiales de datos. (Ley Orgánica de Protección de Datos Personales, 2021)

Este principio, como el de pertinencia y minimización de datos personales guardan estrecha relación y función ya que ambos buscan reducir el campo de acción que tiene el responsable en las actividades que desempeña con los datos personales. Por un lado, la pertinencia y minimización están relacionados con el momento de la recopilación de datos personales,

mientras que el de proporcionalidad limita su tratamiento al establecer estas características básicas del tratamiento.

En este sentido, el limitar el tratamiento de datos personales a criterios lógicos que eviten la vulneración de los derechos paralelos de privacidad e intimidad es una herramienta de prudencia, evitando que con un tratamiento excesivo, inadecuado, irrelevante o inexacto de los datos se atenten garantías legales y contractuales del titular.

### **3.2.7. Principio de confidencialidad. –**

El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.

Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio. (Ley Orgánica de Protección de Datos Personales, 2021)

En similares términos que los del CJI, la confidencialidad se traduce a la prohibición de divulgar y las solas excepciones deben estar determinadas en la Ley. La comunicación de datos personales solo puede darse bajo los términos por los que el titular otorgó su consentimiento cuando los datos fueron recopilados informadamente, o bien, que el titular manifieste su consentimiento para un nuevo tratamiento de datos personales.

### **3.2.8. Principio de calidad y exactitud. –**

Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales.

Siempre que el responsable del tratamiento haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, no le será imputable la

inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

- a) Hubiesen sido obtenidos por el responsable directamente del titular.
- b) Hubiesen sido obtenidos por el responsable de un intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario que recoja en nombre propio los datos de los afectados para su transmisión al responsable.
- c) Fuesen obtenidos de un registro público por el responsable. (Ley Orgánica de Protección de Datos Personales, 2021)

Anteriormente se abarcó el deber del responsable de datos personales de tenerlos actualizados periódicamente. Adicionalmente, el principio de calidad y exactitud ha sido planteado en la LOPDP a su vez como una garantía de la calidad de los datos personales desde el momento de su recopilación. Este principio, como se constató con los principios del CJI, tiene la intención de dotar al titular de la posibilidad de solicitar una corrección de los datos sin necesidad de activar todo el aparataje judicial como en el caso de una acción de habeas data.

Una gran diferencia con el principio de exactitud del CJI es que, en la LOPDP la exactitud tiene tres causales por las que el responsable deviene inimputable de responsabilidad en relación con la exactitud de los datos, los cuales son bastante lógicos, ya que resulta inconcebible que se responsabilice al responsable por obtener datos que son inexactos a costas del titular, que hubiesen sido obtenidos por un intermediario en los casos que aplica, puesto que en tal escenario la responsabilidad debería recaer en el intermediario y no en el nuevo responsable, y finalmente cuando sean obtenidos de registros públicos. La lógica detrás de esta última causa podría fundamentarse en que, al ser registros públicos, se entienden conocidos por el titular y, tanto la naturaleza de confidencialidad de los datos personales no aplicaría en dicho supuesto o bien, que se entienden conocidos por el titular y le corresponde a aquel su rectificación, corrección o actualización.

### **3.2.9. Principio de Conservación. –**

Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento.

Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica.

La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias, para salvaguardar los derechos previstos en esta norma.

La conservación debe entenderse como el límite en el tiempo que tienen los responsables de poder almacenar los datos con el propósito establecido en la convención que llevó al titular a dar su consentimiento. A diferencia de cómo ha sido planteada la conservación limitada por el CJI, la LOPDP se limita a únicamente referirse al acto de la conservación, mientras que los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales abarcaron el tratamiento limitado.

Es menester destacar la diferencia notoria entre conservación y tratamiento de datos personales. A nivel interamericano se consideró limitar ambos aspectos, enfatizando la importancia de vincular el tratamiento al cumplimiento del propósito por los cuales los datos personales fueron recopilados en primer lugar. Por su lado, el legislador ecuatoriano ha obviado este particular y ha optado por hacer que este principio en particular limite únicamente a la conservación de datos personales.

Adicionalmente, el Principio de Conservación de la LOPDP también considera la utilidad de conservar datos para fines de investigación científica, histórica y estadística; en otras palabras, utilidad pública siempre que se establezcan garantías para proteger los datos personales. A esto sería apropiado recalcar que, lo que se ha considerado en instancias internacionales ha sido resguardar tales datos a través de la anonimización.

### **3.2.10. Principio de seguridad de datos personales. –**

Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto. (Ley Orgánica de Protección de Datos Personales, 2021)

Los términos utilizados en este principio guardan mucha similitud con el principio de seguridad de los datos que plantea el CJI. A las medidas de seguridad adecuadas de la LOPDP, los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales los catalogan como salvaguardias, y en ambas premisas se evidencia que este principio se basa en imponer a los responsables y los encargados el deber de tener los datos personales a buen resguardo, sea cual fuere el soporte en el que se encuentran almacenados o guardados y que se atienda a la naturaleza de los datos sensibles con medidas de seguridad (salvaguardias) más apropiadas y estrictas para evitar una vulneración a los soportes o sistema en los que se encuentren almacenados los datos a toda costa.

### **3.2.11. Principio de responsabilidad proactiva y demostrada. –**

El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.

El responsable del tratamiento de datos personales está obligado a rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales.

El responsable del tratamiento de datos personales deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la presente Ley. (Ley Orgánica de Protección de Datos Personales, 2021)

A través de este principio lo que se propone es un mandato a cumplir con los estándares de protección de datos personales y que el responsable pueda demostrarlo. Sin embargo, este principio debe ser considerado una corresponsabilidad para con el Estado, en la medida en que éste debe a su vez tener un control y regulación proactivos y la promoción de incentivos a favor de los responsables, de tal manera que la responsabilidad proactiva devenga un medio de tratar los datos personales y no solo un objetivo y un deber de los responsables.

En lo que concierne al principio de responsabilidad a nivel del CJI, la responsabilidad en la LOPDP es un término que abarca un ámbito de regulación mucho más amplio. Mediante este principio se materializa la obligación y la capacidad coactiva de las Autoridad de Protección de Datos Personales, toda vez que esta responsabilidad tiene muchos mandatos de optimizar las prácticas en cuanto a la arquitectura de los sistemas y herramientas utilizadas para el tratamiento de datos personales, y en correlación con el principio de seguridad de datos personales, los responsables tienen este llamado a adaptar sus herramientas de recopilación y tratamiento a las necesidades del titular.

### **3.2.12. Principio de Aplicación Favorable al Titular. –**

En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.

El ordenamiento jurídico ecuatoriano se ha caracterizado por reconocer las relaciones de poder que existen entre los sujetos de las relaciones jurídico normativas. No es extraño ver en otras ramas del Derecho principios que persiguen minimizar esa brecha entre tales relaciones de poder, tales como el principio de duda a favor del reo en Materia Penal recogido en el artículo 5 numeral 3 del Código Orgánico Integral Penal (Código Orgánico Integral Penal, 2014), o el principio de aplicación favorable al trabajador en el Derecho Laboral establecido en el artículo 7 del Código del Trabajo (Código del Trabajo, 2005).

Este fenómeno ha sido considerado por el legislador ecuatoriano en materia de protección de datos personales también. Sin duda algo novedoso y que no se ha observado en los instrumentos internacionales que han sido objeto de análisis de la presente investigación.

Con el principio de aplicación favorable al titular, lo que se pretende afianzar es una relación más equitativa entre los responsables de datos personales, quienes son custodios de los datos personales y, por ende, sobre quienes pesa la responsabilidad de proteger sus derechos mediante el cumplimiento de las disposiciones normativas contenidas en la LOPDP.

Sin embargo, este principio no va encaminado a que los cumplan los responsables en el tratamiento de datos, si no a los operadores de justicia y a las entidades administrativas. Esto sin duda es demuestra un gran progreso en el accionar legislativo de Ecuador porque la perspectiva del legislador es la del porqué de la norma.

Se ha mencionado anteriormente que la LOPDP nace con el objetivo de garantizar el derecho de la protección de datos personales establecido en la Constitución de la República, y este enfoque más realista de legislar mirando al titular de los derechos que se pretenden amparar en caso de duda sobre el alcance de las normas jurídicas y contractuales en la materia materializa precisamente la razón de ser de la LOPDP.

### **3.2.13. Principio de Independencia del Control. –**

Para el efectivo ejercicio del derecho a la protección de datos personales, y en cumplimiento de las obligaciones de protección de los derechos que tiene el Estado, la Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción. (Ley Orgánica de Protección de Datos Personales, 2021)

Este principio evidentemente es inspirado por el principio trece de los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. En ambos escenarios lo que se propone es el establecimiento de una autoridad de control independiente, imparcial y autónomo. Oportunamente se destacó que esta independencia y autonomía debe ser efectiva, sobre todo en los casos en los que el responsable de los datos personales es el propio Estado, de esta manera se evitan injerencias de los poderes públicos en las garantías que deben ser veladas por la autoridad de control.

### **3.3. Conclusiones**

Con el análisis de cada uno de los principios planteados dentro de los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales se puede concluir lo siguiente:

- Las iniciativas de dar guía a la promulgación de principios sobre la privacidad y la protección de datos se han llevado a cabo por organismos internacionales desde hace más de 30 años antes de la adopción de la Ley Orgánica de Protección de Datos Personales, a partir de la Resolución 45/95 de la Asamblea General de las Naciones Unidas que fue aprobada en 1990.
- Los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales del Comité Jurídico Interamericano de la Organización de Estados Americanos inspiraron considerablemente la formulación de los principios establecidos en la Ley Orgánica de Protección de Datos Personales de Ecuador.
- Mientras que los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales tienen un enfoque mucho más centralizado en el consentimiento de los titulares de datos personales, los principios de la Ley Orgánica de Protección de Datos

Personales de Ecuador tienen un enfoque más centralizado en la responsabilidad del responsable de los datos personales.

- La adopción de instrumentos normativos a nivel interamericano que contemplen las pautas y lineamientos recogidos en los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales permitirá que una mejor tutela de los derechos de los titulares en los casos de flujo transfronterizo de datos personales.

#### **3.4. Críticas y recomendaciones. –**

- El Ecuador debería haber incorporado al flujo transfronterizo de datos como otro principio rector de la Ley Orgánica de Protección de Datos Personales en los términos que plantea el Comité Jurídico Interamericano, de manera que se armonicen los casos en los que los datos no son gestionados en soportes que se encuentren en territorio nacional o exista transferencia de responsabilidad a personas sometidas a otra jurisdicción territorial.
- El legislador ecuatoriano ha hecho una excelente incorporación de los principios y estándares internacionales en su normativa nacional, adecuando las necesidades de una sociedad en constante desarrollo a los estándares internacionales en la materia. A su vez, la integración regional en materia de protección de datos personales es un planteamiento mucho más viable con la adopción de iniciativas que buscan la armonización de las garantías fundamentales de los individuos.
- Ecuador ha hecho un trabajo prolijo en incorporar el principio de aplicación favorable al titular. Esto permite forjar una relación más equitativa, posicionando al titular de los datos personales y del derecho a la protección de datos de carácter personal en una posición menos desventajosa en casos de duda del alcance de las disposiciones normativas en la materia.
- La Asamblea Nacional debería haber tomado en consideración dentro de la LOPDP el tratamiento limitado dentro del principio de conservación en los mismos términos que el CJI, pues el principio de conservación no hace referencia a límites en cuanto al tratamiento de datos personales y su relación con el consentimiento del titular, únicamente se remite al límite en su conservación.
- El legislador planteó el principio de juridicidad en la LOPDP en una forma particular e innovadora al no limitar la aplicación de las normas relativas a protección de datos personales que han sido adoptadas nivel nacional, si no que a modo de clausula abierta, establece la posibilidad de aplicar instrumentos internacionales sobre protección de datos personales, evidentemente, en estricta observancia al resto de



principios de este cuerpo normativo y las disposiciones constitucionales relativas a la materia.

## Referencias

### Normativa

Carta de la Organización de Estados Americanos, (1948).

<https://www.cidh.oas.org/basicos/carta.htm>

Código del Trabajo, (2005). [https://www.trabajo.gob.ec/wp-](https://www.trabajo.gob.ec/wp-content/uploads/downloads/2012/11/Código-de-Tabajo-PDF.pdf)

[content/uploads/downloads/2012/11/Código-de-Tabajo-PDF.pdf](https://www.trabajo.gob.ec/wp-content/uploads/downloads/2012/11/Código-de-Tabajo-PDF.pdf)

Código Orgánico Integral Penal, (2014). [https://www.defensa.gob.ec/wp-](https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf)

[content/uploads/downloads/2018/03/COIP\\_feb2018.pdf](https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf)

Constitución de la República del Ecuador, (2008). [https://www.defensa.gob.ec/wp-](https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf)

[content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador\\_act\\_ene-2021.pdf](https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf)

Constitución Política de Colombia, (1991).

<https://www.cijc.org/es/NuestrasConstituciones/COLOMBIA-Constitucion.pdf>

Constitución Política de la República del Ecuador, (1996).

<https://pdba.georgetown.edu/Constitutions/Ecuador/ecuador96.html#mozTocId928875>

Constitución Política de la República del Ecuador, (1998). [https://www.cancilleria.gob.ec/wp-](https://www.cancilleria.gob.ec/wp-content/uploads/2013/06/constitucion_1998.pdf)

[content/uploads/2013/06/constitucion\\_1998.pdf](https://www.cancilleria.gob.ec/wp-content/uploads/2013/06/constitucion_1998.pdf)

Declaración Universal de Derechos Humanos, (1948). [https://www.un.org/es/about-](https://www.un.org/es/about-us/universal-declaration-of-human-rights)

[us/universal-declaration-of-human-rights](https://www.un.org/es/about-us/universal-declaration-of-human-rights)

General Assembly Resolution 45/95, Guidelines for the regulation of computerized personal

data files, (1990). [https://digitallibrary.un.org/record/105299/files/A\\_RES\\_45\\_95-EN.pdf?ln=en](https://digitallibrary.un.org/record/105299/files/A_RES_45_95-EN.pdf?ln=en)

General Assembly Resolution 68/167. The right to privacy in the digital age, (2013).

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/47/PDF/N1344947.pdf?OpenElement>

Ley 1266 de 2008, (2008).

<https://www.oas.org/es/sla/ddi/docs/CO%2014%20Ley%201266%20Habeas%20Data.pdf>

Ley de Control Constitucional, (1997). <https://docs.ecuador.justia.com/nacionales/leyes/ley-de-control-constitucional.pdf>

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, 5/1992 (1992).

<https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189>

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, (2009).

[https://www.oas.org/juridico/PDFs/mesicic4\\_ecu\\_org2.pdf](https://www.oas.org/juridico/PDFs/mesicic4_ecu_org2.pdf)

Ley Orgánica de Protección de Datos Personales, (2021).

<https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf>

Organización de Estados Americanos. (2022). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales*. Departamento de Derecho Internacional OEA.

[https://www.oas.org/es/sla/cji/docs/Publicacion\\_Proteccion\\_Datos\\_Personales\\_Principios\\_Actualizados\\_2021.pdf](https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf)

Red Iberoamericana de Protección de Datos. (2017). *Estándares de Protección de Datos Personales*. [https://www.redipd.org/sites/default/files/inline-](https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf)

[files/Estandares\\_Esp\\_Con\\_logo\\_RIPD.pdf](https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf)

Resolution 28/16. The right to privacy in the digital age, (2015). <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/068/78/PDF/G1506878.pdf?OpenElement>

Spain (Ed.). (2018). *Constitución española* (Quinta edición). Agencia Estatal Boletín Oficial del Estado.

## Tesis

Cabezas Mena, D. F., & Lucas Franco, G. E. (2023). *Análisis Comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la Legislación Española desde un enfoque de ciberseguridad y delitos informáticos* [Tesis de Posgrado, Universidad Politécnica Salesiana].

<https://dspace.ups.edu.ec/bitstream/123456789/25114/1/UPS-CT010600.pdf>

Clímaco Valiente, H. (2012). *Génesis histórico-normativa del derecho a la protección de los datos personales desde el derecho comparado a propósito de su fundamento* [Tesina, Universidad Carlos III de Madrid]. [https://e-archivo.uc3m.es/bitstream/handle/10016/18785/TFM\\_MEADH\\_Ernesto\\_Climaco.pdf?sequence=1&isAllowed=y](https://e-archivo.uc3m.es/bitstream/handle/10016/18785/TFM_MEADH_Ernesto_Climaco.pdf?sequence=1&isAllowed=y)

### Artículos e informes

Caldas, M. (2022, julio 26). *PRINCIPIOS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. <https://globalsupport.com.ec/2022/07/26/principios-de-la-ley-organica-de-proteccion-de-datos-personales/#:~:text=Juridicidad%2C%20es%20decir%2C%20el%20apego,la%20relación%20con%20el%20titular.>

González Porras, A. J. (2015). *PRIVACIDAD EN INTERNET: Los derechos fundamentales de privacidad e intimidad en Internet y su regulación jurídica. La vigilancia masiva*. [Universidad de Castilla-La Mancha]. <https://ruidera.uclm.es/xmlui/bitstream/handle/10578/10092/TESIS%20Gonz%c3%a1lez%20Porras.pdf?sequence=1&isAllowed=y>

Ministerio de Relaciones Exteriores y Movilidad Humana. (2020). *Ecuador, primer país del mundo en ratificar los 27 tratados de Naciones Unidas sobre derechos humanos*.

Naranjo Godoy, L. (2021). *El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador*. <https://revistas.uasb.edu.ec/index.php/foro/article/view/501/2419#info>

Office of the United Nations High Commissioner for Human Rights. (2023). *International standards, OHCHR and privacy in the digital age*. <https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards>

Red Iberoamericana de Protección de Datos. (2020). *PLAN ESTRATÉGICO 2021-2025*. <https://www.redipd.org/sites/default/files/2020-12/Plan-Estrategico-RIPD-2021-2025.pdf>

Red Iberoamericana de Protección de Datos. (2023, julio 23). *Historia de la Red Iberoamericana de Protección de Datos (RIPD)* [Institucional]. <https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd>

Rojas Bejarano, M. (2014). *Evolución del derecho de protección de datos personales en Colombia*. <https://novumjus.ucatolica.edu.co/article/download/652/670>

United Nations Development Programme. (2023). *UNDP GUIDE - DRAFTING DATA PROTECTION LEGISLATION: A STUDY OF REGIONAL FRAMEWORKS*.  
<https://www.undp.org/sites/g/files/zskgke326/files/2023-04/UNDP%20Drafting%20Data%20Protection%20Legislation%20March%202023.pdf>

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220. <https://www.jstor.org/stable/1321160?seq=2>

## **Sentencias**

Sentencia C-334/10, (12 de mayo de 2010).

<https://www.corteconstitucional.gov.co/relatoria/2010/C-334-10.htm>

Sentencia C-748/11, (6 de octubre de 2011).

<https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm>

Sentencia No. SU-082/95, (3 de marzo de 1995).

<https://www.corteconstitucional.gov.co/relatoria/1995/su082-95.htm>

Sentencia No. T-414/92, (16 de junio de 1992).

<https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm>

Sentencia T-729/02, (5 de septiembre de 2002).

<https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm>