



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TEMA:

**“La eficacia de la protección constitucional de los datos personales frente a los delitos
informáticos en Ecuador”**

AUTORES:

Vega Narvaez Belén Elizabeth

Pacheco Mendoza Aquiles Melquiades

Trabajo de titulación previo a la obtención del título de

ABOGADO

TUTOR:

Dra. Ramírez Vera María Paula

Guayaquil, Ecuador

23 de agosto del 2026



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por

VEGA NARVAEZ BELÉN ELIZABETH; PACHECO MENDOZA AQUILES

MELQUIADES, como requerimiento para la obtención del título de Abogado.

TUTOR



firmado electrónicamente por:
**MARIA PAULA
RAMIREZ VERA**

DRA. MARÍA PAULA RAMÍREZ VERA

DIRECTORA DE LA CARRERA

f. _____

Dra. NURIA PEREZ PUIG-MIR, PHD

Guayaquil, a los 23 del mes de agosto del año 2026



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, Vega Narvaez Belén Elizabeth y Pacheco Mendoza Aquiles Melquiades

DECLARAMOS QUE:

El Trabajo de Titulación, **“LA EFICACIA DE LA PROTECCIÓN CONSTITUCIONAL DE LOS DATOS PERSONALES FRENTE A LOS DELITOS INFORMÁTICOS EN ECUADOR”** previo a la obtención del título de Abogado, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente, este trabajo es de nuestra total autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 23 del mes de agosto del año 2026

LOS AUTORES

f. _____

VEGA NARVAEZ BELÉN ELIZABETH

f. _____

PACHECO MENDOZA AQUILES MELQUIADES



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

AUTORIZACIÓN

Nosotros, Vega Narvaez Belén Elizabeth y Pacheco Mendoza Aquiles Melquiades

Autorizamos a la Universidad Católica Santiago de Guayaquil a la publicación en la biblioteca de la institución del Trabajo de Titulación **“LA EFICACIA DE LA PROTECCIÓN CONSTITUCIONAL DE LOS DATOS PERSONALES FRENTE A LOS DELITOS INFORMÁTICOS EN ECUADOR”** cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 23 del mes de agosto del año 2026

LOS AUTORES

f. _____

VEGA NARVAEZ BELÉN ELIZABETH

f. _____

PACHECO MENDOZA AQUILES MELQUIADES



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

REPORTE COMPILATIO:



Certificado de análisis

Compilatio Magister+ | UCSG-EC- Universidad Católica de Santiago de Guayaquil

TEMA UTE AQUILES Y BELEN PROYECTO FINAL 23 DE AGOSTO DEL AÑO 2026

ID : 6b22ce417cbe27749326202e5e9d80e41ef43809



<1%

Textos sospechosos

Nombre del fichero : TEMA UTE AQUILES Y BELEN PROYECTO FINAL 23 DE AGOSTO DEL AÑO 2026.txt
Tamaño del archivo original : 105,3 kB
Número de palabras : 16.252

Depositante : María Paula Ramírez
Fecha de depósito : 20 de agosto de 2026
Tipo de carga : interface
fecha de fin de análisis : 20 de agosto de 2026

Resumen (sección 1/2)

Localización de los textos sospechosos en el documento :



Incluido en el porcentaje de textos sospechosos :



Similitudes

<1%

Pasajes con similitudes a fuentes encontradas en diferentes colecciones.



Detección de IA

34%

Textos estilísticamente próximos a un texto generado por una IA.

Este índice es un indicador y no una prueba. Comprueba con el autor si domina los conocimientos mencionados en el documento.



Idiomas no reconocidos

2%

Pasajes en los que parte del vocabulario utilizado no forma parte del diccionario de la lengua.

Puede tratarse de un intento del autor de modificar el texto para evitar ser detectado.



No incluido en el porcentaje de textos sospechosos :



Textos entre comillas

1%

Pasajes entre comillas, a menudo indicativos de una cita.

Similitudes

<1%

Párrafos con similitudes a fuentes encontradas en diferentes colecciones.



Fuente principal detectada

N°		Descripciones	Similitudes	Ubicaciones
1		La acción afirmativa y el empoderamiento de las mujeres en... localhost/mba/bitstream/33131/4588/3/T-UCSG-PRE-JUR-DIR-551.pdf.txt	1%	
2		Incidencia del Grooming en el Ecuador y regulación en el COIP... localhost/mba/bitstream/33131/4584/3/T-UCSG-PRE-JUR-DIR-543.pdf.txt	1%	
3		Vulneración del derecho a la seguridad social del trabajador bajo... localhost/mba/bitstream/33131/4636/3/T-UCSG-PRE-JUR-DIR-677.pdf.txt	1%	
4		Débiles informáticos: un análisis jurídico integral de las amenazas... dispace.upsi.edu.ec/bitstream/123456789/30252	<1%	
5		Presentación Tiza y Pizarra Genially view.genially.com/55b18cfbeedc950316c4636/presentation-presentacio...	<1%	
6		Tratados bilaterales de inversiones, denuncias efectuadas por el... repositorio.uscg.edu.ec/bitstream/33131/4608/1/T-UCSG-PRE-JUR-DIR-68...	<1%	
7		Documento de otro usuario: anuar Viene de de otro grupo	<1%	
8		Quinto Avanza, Pérez Rivera María Fernanda Viene de de no biblioteca	<1%	
9		Los delitos informáticos y su afectación sobre los bienes jurídicos... localhost/mba/bitstream/33131/4643/3/T-UCSG-PRE-JUR-DIR-MD-196.pdf...	<1%	
10		Documento de otro usuario: anuar Viene de de otro grupo	<1%	

Fuente mencionada (sin similitudes detectadas)

N°		Descripciones
1		https://www.argentina.gob.ar/normativa/nacional/decreto-1558-2001-70368
2		https://www.bcn.cl/leychile/navegar/?idNorma=141599
3		https://www.bcn.cl/leychile/navegar/?idNorma=1206272
4		https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488
5		https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=48981

Nº		Descripciones
6		https://www.funcionpublica.gob.es/eva/gendormativo/norma.php?i=53646
7		https://sacc.corteconstitucional.gob.es/storage/api/v1/10_DWS_FL/wyY(YX)wZ0RhjpsaHhjbW02ZS1uWV1aW...
8		https://revistas.usach.edu.ec/index.php/foro/articulos/view/500/487
9		https://www.bce.es/lstcom/art.php?id=BCE-A-2018-16673
10		https://www.fiscalia.gob.es/analitica-noticias-del-delito/
11		https://www.fiscalia.gob.es/wp-content/uploads/2025/01/Política-Criminal-de-Cibercriminalidad.pdf
12		https://revistas.usach.edu.ec/index.php/foro/articulos/view/501/488
13		https://doi.org/10.81243/calams.13.156
14		https://eur-lex.europa.eu/eli/reg/2016/575/oj/0ocalames
15		https://sacc.corteconstitucional.gob.es/storage/api/v1/10_DWS_FL/wyY(YX)wZ0RhjpsaHhjbW02ZS1uWV1aW...



Firmado electrónicamente por:
**MARIA PAULA
RAMIREZ VERA**

DEDICATORIA

Yo, Belén Elizabeth Vega Narváez, dedico este trabajo a Dios, por darme la fortaleza para continuar este camino.

A mis padres y a mi familia, por su amor, apoyo y confianza incondicional. Este logro es también fruto de todo lo que han hecho por mí.

Y en especial a mi tío, el Dr. Carlos Manuel Narváez Zambrano, quien en vida me enseñó este mundo del derecho y agradezco cada aprendizaje que tuve gracias a sus conocimientos.

DEDICATORIA

Yo, Aquiles Melquiades Pacheco Mendoza, A mi Padre Celestial y a mi Madre del Cielo, la Santísima Virgen María, por guiarme, fortalecerme y acompañarme siempre.

A mis queridos abuelitos y, de manera especial, a mis padres Mercedes Mendoza y Aquiles Pacheco, quienes, aunque ya no están físicamente conmigo, viven eternamente en mi corazón. Este logro es también para ustedes.

A mi esposa Jackeline, a mis hijos Stephany, Aquiles, James e Ian, a mis ocho nietos, a mis tíos, a mi hermano Ricardo, a mis nueras y a mi yerno, por su amor y por ser parte fundamental de mi vida.

Con todo mi amor y gratitud, dedico este logro a ustedes.



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO



Firmado electrónicamente por:
**MARIA PAULA
RAMIREZ VERA**

DRA. MARÍA PAULA RAMÍREZ VERA

TUTOR

f. _____

DRA. NURIA PÉREZ PUIG-MIR. MGS.

PHD DIRECTORA DE CARRERA DE

DERECHO

f. _____

DR. XAVIER ZAVALA EGAS

DECANO

f. _____

.....



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Facultad: Jurisprudencia
Carrera: Derecho
Periodo: Semestre A2026
Fecha: 20 de agosto de 2026.

ACTA DE INFORME FINAL

La abajofirmante, docente tutora del Trabajo de Titulación denominado ***La eficacia de la protección constitucional de los datos personales frente a los delitos informáticos en Ecuador*** elaborado por los estudiantes ***VEGA NARVAEZ BELÉN ELIZABETH y PACHECO MENDOZA AQUILES MELQUIADES***, certifica que durante el proceso de acompañamiento dicha estudiante han obtenido la calificación de ***8.5/10 (ocho cincuenta sobre diez)***, lo cual los califica como ***APTOS PARA LA SUSTENTACIÓN***.



Clave de verificación: 0001
**MARIA PAULA
RAMIREZ VERA**
08/08/2026

**Abg. María Paula Ramírez, Mgs.
Docente Tutora.**

OPONENTE

Indice

CAPÍTULO I.....	2
Planteamiento del problema.....	2
Delimitación del problema jurídico.....	4
Justificación.....	6
Objetivos	7
Objetivo general	7
Objetivos específicos.....	7
CAPÍTULO II	8
Marco teórico	8
2.1. Derecho a la protección de datos personales.....	8
2.2. Principios y derechos de la protección de datos personales	12
2.3. Regulación jurídica de la protección de datos personales en el Ecuador	15
2.4. Protección de los datos personales frente a los delitos informáticos.....	21
2.5. Eficacia de la protección jurídica frente a los delitos informáticos.....	28
2.5.1 Derecho comparado: experiencias de España, Colombia, Argentina y Chile.....	30
2.5.2 Eficacia institucional en la protección de los datos personales	34
2.5.3 Análisis crítico de la protección jurídica de los datos personales frente a los delitos informáticos.....	35

2.6 Desarrollo Jurisprudencial.....	39
2.7 Propuesta jurídica orientada a fortalecer los mecanismos de protección constitucional de los datos personales frente a los delitos informáticos en el Ecuador	43
2.7.1 Protocolo de coordinación interinstitucional entre la Superintendencia de Protección de Datos Personales, la Fiscalía General del Estado y la Policía Nacional	43
2.7.2 Facultad de investigación y auditoría de oficio de la Superintendencia de Protección de Datos Personales.....	46
2.7.3 Elementos complementarios.....	48
CAPÍTULO III	49
Metodología	49
3.1 Enfoque de investigación	49
3.2 Tipo y alcance de la investigación.....	49
3.3 Métodos de investigación	50
3.3.1 Método jurídico-dogmático.....	50
3.3.2 Método analítico.....	51
3.3.3 Método hermenéutico jurídico	51
3.3.4 Método comparado.....	51
3.3.5 Corpus documental y criterios de selección de fuentes.....	51
3.4 Técnicas e Instrumentos de investigación	53
3.5 Procedimiento metodológico.....	54

CAPÍTULO IV	54
Conclusiones	54
Bibliografía.....	55

RESUMEN

La presente investigación analizó la eficacia de la protección constitucional de los datos personales frente a los delitos informáticos en el Ecuador, considerando las garantías constitucionales y el marco jurídico vigente. Se empleó un enfoque cualitativo, con alcance descriptivo, analítico y propositivo, mediante los métodos jurídico-dogmático, analítico, hermenéutico jurídico y comparado. Para ello, se examinó la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, el Código Orgánico Integral Penal, la jurisprudencia constitucional y referentes normativos de España, Colombia, Argentina y Chile. Los resultados evidenciaron que, aunque Ecuador cuenta con una base constitucional y legal importante, persisten dificultades en materia de prevención, investigación y coordinación institucional. En particular, se identificó la necesidad de fortalecer la articulación entre la Superintendencia de Protección de Datos Personales, la Fiscalía General del Estado y la Policía Nacional. Como respuesta, se planteó un protocolo de coordinación interinstitucional y el fortalecimiento de las facultades de la Superintendencia para realizar investigaciones y auditorías de oficio en sectores de mayor riesgo. Se concluye que es necesario reforzar los mecanismos preventivos e institucionales para garantizar una protección más efectiva de los datos personales frente a los delitos informáticos.

Palabras claves: Delitos informáticos, tutela efectiva, eficacia jurídica, prevención, vulneración de derechos, supervisión y control

CAPÍTULO I

Planteamiento del problema

¿En qué medida las garantías constitucionales y el marco jurídico vigente en Ecuador garantizan una protección efectiva del derecho a la protección de los datos personales frente a los delitos informáticos?

El acelerado proceso de transformación digital experimentado por el Ecuador ha incrementado significativamente el intercambio y almacenamiento de datos personales en plataformas tecnológicas utilizadas por instituciones públicas, empresas privadas y ciudadanos. Esta realidad ha favorecido el desarrollo económico y social; sin embargo, también ha incrementado la exposición de la información personal a nuevas modalidades de ciberdelincuencia que afectan directamente el derecho fundamental a la protección de datos personales

De acuerdo con la información proporcionada por la Fiscalía General del Estado, durante el período comprendido entre agosto de 2014 y julio de 2025 se registraron 8.256 noticias del delito relacionadas con delitos informáticos a escala nacional. Estos datos evidencian una tendencia ascendente en este tipo de infracciones y permiten advertir la relevancia de analizar la protección de los datos personales frente a las conductas delictivas desarrolladas mediante medios tecnológicos (Fiscalía General del Estado, 2025).

También, la Política Criminal de Ciberdelincuencia de la Fiscalía General del Estado (2026) señala que entre agosto de 2014 y julio de 2025 se registraron 8.256 noticias del delito relacionadas con delitos informáticos, evidenciando una tendencia creciente en este tipo de infracciones.

Estas conductas pueden afectar tanto a personas naturales como a instituciones públicas y privadas, ocasionando perjuicios económicos y comprometiendo derechos fundamentales relacionados con la privacidad, la intimidad y la protección de los datos personales. La problemática también ha sido reconocida por la Corte Constitucional del Ecuador (2021) mediante la sentencia No. 2064-14-EP, de 27 de enero de 2021, en la que analizó un caso relacionado con la conservación y posesión de fotografías íntimas y personales sin el consentimiento de su titular. Al resolver el caso, la Corte determinó la vulneración de los derechos constitucionales a la protección de datos personales y a la autodeterminación informativa, así como de los derechos a la imagen, a la honra, al buen nombre y a la intimidad.

Este precedente evidencia que el tratamiento indebido de datos personales puede ocasionar graves afectaciones a los derechos fundamentales de las personas y demuestra que los riesgos asociados al uso indebido de la información personal no solo se presentan en el ámbito privado, sino que también pueden materializarse mediante conductas vinculadas al entorno digital y a los delitos informáticos. En consecuencia, resulta necesario analizar si el marco constitucional y legal vigente en el Ecuador ofrece una protección efectiva frente a estas amenazas.

A pesar de que el ordenamiento jurídico ecuatoriano reconoce el derecho a la protección de datos personales en el artículo 66, numeral 19, de la Constitución de la República del

Ecuador, cuenta con la Ley Orgánica de Protección de Datos Personales y contempla diversas disposiciones en el Código Orgánico Integral Penal, persisten desafíos para garantizar una protección efectiva de este derecho. Esta situación plantea posibles desafíos relacionados con la cultura de protección de datos, la complejidad para investigar los delitos informáticos y las posibles limitaciones prácticas en la aplicación de los mecanismos legales existentes.

En consecuencia, el crecimiento de la ciberdelincuencia no solo representa un problema de seguridad informática, sino también un desafío para la eficacia de la protección constitucional de los datos personales. Esta situación justifica la necesidad de analizar si el marco jurídico ecuatoriano ofrece una respuesta suficiente frente a las nuevas formas de vulneración de la información personal o si resulta necesario fortalecer los mecanismos de prevención, protección y sanción existentes.

A pesar de la vigencia de la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales y las disposiciones del Código Orgánico Integral Penal, podrían existir limitaciones prácticas que incidan en la protección efectiva de los datos personales. La naturaleza transnacional de los delitos informáticos, la constante evolución de las tecnologías empleadas para su comisión y la dificultad para identificar a sus responsables complican la prevención e investigación de estas conductas. Asimismo, la obtención, preservación y valoración de la evidencia digital requiere conocimientos técnicos especializados y mecanismos de cooperación, cuya disponibilidad y aplicación constituyen aspectos que fueron analizados en esta investigación en relación con la eficacia de la investigación penal. Naranjo Godoy (2017)

A ello podrían sumarse posibles desafíos institucionales relacionados con la coordinación entre las entidades encargadas de garantizar la protección de los datos personales y aquellas responsables de investigar y sancionar los delitos informáticos. Aunque el ordenamiento jurídico ecuatoriano reconoce este derecho fundamental y establece obligaciones para los responsables del tratamiento de datos, aún resulta necesario fortalecer la articulación institucional, la especialización técnica y los mecanismos de supervisión para asegurar una respuesta eficaz frente a las nuevas modalidades de ciberdelincuencia. Estas circunstancias justifican la necesidad de analizar críticamente si el marco jurídico vigente garantiza una protección efectiva de los datos personales o si requiere ajustes que permitan responder adecuadamente a los desafíos actuales Naranjo Godoy (2020)

El crecimiento de las conductas delictivas que implican la obtención, utilización o tratamiento ilícito de datos personales constituye no solo un problema de seguridad digital, sino también un desafío para la eficacia de la protección constitucional de este derecho fundamental. Por ello, resulta necesario analizar críticamente si el marco jurídico ecuatoriano garantiza una protección efectiva de los datos personales frente a estas modalidades delictivas o si requiere ajustes normativos e institucionales que fortalezcan los mecanismos de prevención, protección, investigación y sanción.

Delimitación del problema jurídico

La presente investigación delimita su análisis a la relación normativa entre la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, su Reglamento General y el Código Orgánico Integral Penal, en lo relativo a la protección de los

datos personales frente a conductas delictivas que afectan directamente su obtención, utilización y tratamiento en entornos digitales.

Se toman como referentes de análisis el phishing y la suplantación de identidad digital, en tanto modalidades frecuentes mediante las cuales se materializa la vulneración de datos personales, precisando su tratamiento jurídico en la legislación vigente el phishing no se encuentra denominado expresamente como delito autónomo bajo esa denominación en el COIP, pero determinadas conductas que lo integran pueden encontrarse comprendidas en tipos penales específicos, particularmente en el artículo 230, numeral 2 respecto de su fase de engaño técnico y, según el resultado producido, en el artículo 190 cuando existe apropiación fraudulenta por medios electrónicos; mientras que la suplantación de identidad sí se encuentra tipificada de manera autónoma en el Art. 212 del COIP, sin que la norma distinga expresamente una modalidad digital, lo que genera dificultades de aplicación e interpretación cuando dicha conducta se comete a través de medios electrónicos.

La falencia específica que fue objeto de análisis consiste en determinar si el marco jurídico vigente integrado por la Constitución, la Ley Orgánica de Protección de Datos Personales, su Reglamento General y el Código Orgánico Integral Penal, presenta limitaciones para garantizar una protección efectiva de los datos personales frente a estas conductas, así como establecer si existe una adecuada articulación entre dichos cuerpos normativos para prevenir, investigar, sancionar y reparar las vulneraciones a este derecho fundamental.

La investigación examinó si el reconocimiento constitucional del derecho a la protección de los datos personales, previsto en el artículo 66, numeral 19, de la Constitución de la República del Ecuador, cuenta con mecanismos legales suficientes que permitan garantizar una tutela

efectiva frente a estas modalidades delictivas, o si resulta necesario fortalecer la coordinación y aplicación de la normativa vigente.

Justificación

La presente investigación posee relevancia jurídica, social y académica. Desde el punto de vista jurídico, permite analizar la eficacia de las normas constitucionales y legales destinadas a proteger los datos personales frente a las nuevas modalidades delictivas que surgen en el entorno digital. Asimismo, contribuye a identificar posibles falencias normativas y prácticas que puedan afectar la tutela efectiva de este derecho fundamental.

Desde una perspectiva social, la investigación resulta pertinente debido al incremento de las actividades realizadas mediante medios electrónicos y al aumento de los riesgos asociados al tratamiento indebido de datos personales. La protección de la información personal constituye una necesidad creciente para los ciudadanos, quienes se encuentran cada vez más expuestos a delitos informáticos que pueden ocasionar perjuicios económicos, patrimoniales y morales.

En el ámbito académico, este estudio aportará al desarrollo de la doctrina nacional sobre protección de datos personales y ciberdelincuencia, temas que han adquirido especial importancia en los últimos años debido a la transformación digital de la sociedad. Además, permitirá generar propuestas jurídicas orientadas al fortalecimiento de las garantías constitucionales y legales existentes.

Esta investigación posee utilidad práctica porque sus resultados podrían servir como referencia para futuras reformas legislativas, políticas públicas y mecanismos de protección que

contribuyan a garantizar una tutela más efectiva de los datos personales frente a los delitos informáticos.

Objetivos

Objetivo general

Analizar la suficiencia de los mecanismos de protección constitucional de los datos personales frente a los delitos informáticos en Ecuador, y las limitaciones normativas e institucionales que inciden en su aplicación, con la finalidad de determinar su eficacia y proponer alternativas jurídicas que fortalezcan la tutela de este derecho fundamental.

Objetivos específicos

- Examinar el marco constitucional y legal ecuatoriano que regula la protección de los datos personales y los delitos informáticos, a fin de determinar el alcance de las garantías y mecanismos jurídicos vigentes.
- Identificar las principales limitaciones normativas e institucionales que inciden en la protección de los datos personales frente a los delitos informáticos en el Ecuador.
- Analizar la doctrina, la jurisprudencia y los casos relevantes relacionados con la vulneración de datos personales mediante delitos informáticos, con el propósito de evaluar la aplicación e interpretación del marco jurídico vigente.
- Formular propuestas jurídicas orientadas a fortalecer los mecanismos de protección constitucional de los datos personales frente a los delitos informáticos en el Ecuador.

CAPÍTULO II

Marco teórico

2.1. Derecho a la protección de datos personales

La protección de los datos personales constituye un derecho fundamental autónomo, distinto de aquellos de los que históricamente se desprendió, y guarda una vinculación estrecha con la dignidad humana, la libertad y el libre desarrollo de la personalidad. Su contenido esencial comprende la facultad de toda persona para controlar la información que la identifica o la hace identificable, de modo que pueda conocer, acceder, actualizar, rectificar, limitar o impedir el tratamiento que terceros realicen sobre sus datos. Este derecho adquiere una relevancia particular en la sociedad digital contemporánea, donde el intercambio constante de información a través de medios tecnológicos multiplica los riesgos de uso indebido, comercialización no autorizada o exposición de los datos personales.

A diferencia del derecho a la intimidad, concebido tradicionalmente como una garantía defensiva frente a las injerencias arbitrarias en la esfera privada, el derecho a la protección de datos personales posee una dimensión activa: no se limita a excluir a terceros de un ámbito reservado, sino que atribuye al titular la facultad de decidir sobre la recopilación, el almacenamiento, la utilización y la transferencia de la información que le concierne. Pérez Luño (2012) sostiene que el desarrollo tecnológico ha generado nuevas formas de afectación a los derechos fundamentales, lo que ha obligado a construir mecanismos jurídicos capaces de proteger a la persona frente al uso indebido de su información. En este orden de ideas, Puccinelli (2003) sostiene que la protección de los datos personales reconoce a la persona como titular de un derecho fundamental que le permite ejercer un control efectivo sobre la información que la identifica, superando la concepción tradicional que la consideraba un mero objeto de tratamiento

de datos. Esta evolución explica que los ordenamientos constitucionales contemporáneos hayan reconocido la protección de datos como un derecho autónomo, diferenciado del derecho a la intimidad.

En el ordenamiento jurídico ecuatoriano, este derecho encuentra su fundamento en el artículo 66, numeral 19, de la Constitución de la República, que garantiza a toda persona la protección de sus datos de carácter personal y le reconoce la facultad de conocer, acceder, actualizar, rectificar y decidir sobre el uso que se dé a dicha información. Además del reconocimiento constitucional del derecho a la protección de los datos personales, la Constitución contempla la garantía jurisdiccional del hábeas data, prevista en su artículo 92, mediante la cual toda persona puede acceder a los documentos, bancos de datos e informes que sobre sí misma o sus bienes consten en entidades públicas o privadas, así como solicitar su actualización, rectificación, eliminación o anulación cuando contengan información errónea o afecten ilegítimamente sus derechos. La interpretación conjunta de estas disposiciones evidencia que el marco constitucional no solo reconoce el derecho a la protección de los datos personales, sino que también establece un mecanismo jurisdiccional que permite a las personas protegerlo y exigir su respeto cuando este sea vulnerado.

Este reconocimiento constitucional representa un avance significativo dentro del catálogo de derechos fundamentales, pues incorpora la protección de datos personales como garantía indispensable frente a los riesgos que trae consigo el uso intensivo de las tecnologías de la información. La Corte Constitucional del Ecuador, en la Sentencia No. 2064-14-EP/21 (2021), caso en el que conoció la difusión no consentida de fotografías íntimas mediante una acción de hábeas data, adoptó una noción amplia de dato personal, entendido como toda información que haga referencia directa o indirecta a cualquier aspecto relativo a una persona, y afirmó que el

titular conserva su facultad de control sobre la información incluso después de haber autorizado un tratamiento determinado, pudiendo revocar dicha autorización y exigir su actualización, rectificación o eliminación. Esta línea jurisprudencial confirma que el derecho no se agota en una facultad de exclusión frente a terceros, sino que comprende un haz de facultades de control activo sobre la propia información, en estrecha conexión con el libre desarrollo de la personalidad y con la garantía jurisdiccional del hábeas data.

Uno de los principales fundamentos doctrinales de este derecho es la autodeterminación informativa, entendida como la facultad que posee toda persona para decidir sobre la recopilación, utilización y divulgación de la información relacionada con su identidad. Este concepto tiene su origen en la sentencia emitida por el (Tribunal Constitucional Federal Alemán) en 1983, con ocasión del denominado caso de la Ley del Censo (Volkszählungsurteil), mediante la cual se reconoció que el tratamiento indiscriminado de datos personales puede afectar la libertad individual y la dignidad humana, razón por la cual el individuo debe conservar la capacidad de decidir sobre el uso de su información. Esta sentencia es considerada por la doctrina constitucional comparada, de forma prácticamente unánime, como el origen dogmático de la autodeterminación informativa como categoría autónoma.

Desde la doctrina latinoamericana, Puccinelli (2003) sostiene que la protección de datos personales constituye una evolución del derecho a la intimidad, en tanto responde a la necesidad de dotar a las personas de herramientas jurídicas que les permitan ejercer un control efectivo sobre el tratamiento de su información frente a los riesgos propios del desarrollo tecnológico.

Bajo esta lectura, la autodeterminación informativa transforma al individuo de un sujeto pasivo frente al manejo de sus datos personales en un sujeto activo, con capacidad para conocer, autorizar, limitar y controlar el tratamiento de la información que le concierne. La protección de

datos personales mantiene una relación estrecha con los derechos a la privacidad y a la intimidad, aunque no deben confundirse entre sí. La intimidad protege el ámbito reservado de la vida personal y familiar frente a intromisiones indebidas, mientras que la privacidad abarca un espacio más amplio, vinculado con la capacidad de cada individuo para decidir cuándo, cómo y en qué medida la información sobre su persona puede ser conocida por terceros. Para Westin (1967), lo que hace privada una información no es su contenido sino el control que su titular conserva sobre el momento y el grado en que otros pueden acceder a ella. Esta concepción constituye uno de los pilares sobre los que se ha desarrollado el moderno derecho a la protección de datos personales y ha influido de manera significativa en la doctrina posterior.

En el marco de la transformación digital, la protección de datos personales se vincula también con los denominados derechos digitales, entendidos como la proyección de los derechos fundamentales dentro del entorno tecnológico. Entre ellos destacan el derecho a la identidad digital, el derecho al olvido, el derecho a la desconexión digital y la garantía frente a decisiones automatizadas que produzcan efectos jurídicos sobre la persona sin intervención humana.

Instrumentos como el Reglamento General de Protección de Datos de la Unión Europea (RGPD), el Convenio 108 del Consejo de Europa y la Carta de Derechos Digitales de España dan cuenta de la importancia creciente que el constitucionalismo contemporáneo atribuye a estos derechos, y constituyen un referente de derecho comparado útil para valorar el estado de la regulación ecuatoriana.

El derecho a la protección de los datos personales constituye, en definitiva, una garantía indispensable para preservar la libertad, la dignidad y la autonomía de las personas dentro de la sociedad digital. Su reconocimiento constitucional representa un avance significativo en la tutela de los derechos fundamentales; sin embargo, para que dicha protección resulte realmente

efectiva no basta con declararla en abstracto, sino que se requiere un conjunto de principios y derechos que orienten el tratamiento de la información personal y garanticen su ejercicio efectivo. Corresponde, por ello, examinar los principios rectores y los derechos que conforman el contenido esencial del sistema de protección de datos personales.

En síntesis, estos cinco conceptos no son sinónimos: la intimidad protege el ámbito reservado de la vida personal frente a intromisiones; la privacidad es más amplia y se refiere a la capacidad de decidir qué información propia conocen terceros; la autodeterminación informativa es la facultad de controlar activamente el tratamiento de la propia información; la protección de datos personales es el derecho fundamental autónomo que instrumentaliza esa autodeterminación; y el hábeas data es la garantía jurisdiccional que permite exigirlo en sede judicial. Para efectos de esta investigación, el objeto de estudio es específicamente el derecho a la protección de datos personales y su tutela penal, no la intimidad ni la privacidad en general.

2.2. Principios y derechos de la protección de datos personales

La protección de los datos personales no se agota en su reconocimiento constitucional; requiere un conjunto de principios y derechos que orienten el tratamiento de la información y garanticen al titular un control real sobre ella. Estos elementos constituyen el núcleo del régimen previsto en la Ley Orgánica de Protección de Datos Personales (LOPDP), norma que fija las condiciones bajo las cuales los datos pueden recopilarse, utilizarse, almacenarse y compartirse, siempre con el propósito de resguardar la dignidad, la privacidad y la autodeterminación informativa de las personas. Entre los principios que rigen el tratamiento de los datos personales, el artículo 10 de la LOPDP enumera, en primer término, los de juridicidad, lealtad y transparencia (literales a, b y c), que exigen que toda actividad de tratamiento cuente con una base jurídica válida y que el titular sea informado con claridad sobre la finalidad y las condiciones en que sus datos serán utilizados.

A ellos se suma el principio de finalidad (literal d), que impide recopilar datos para objetivos distintos de los determinados, explícitos y legítimos, y los principios, diferenciados por la propia ley, de pertinencia y minimización de datos personales (literal e), que limita el tratamiento a la información estrictamente necesaria para la finalidad perseguida, y de proporcionalidad del tratamiento (literal f), que exige que este sea adecuado, necesario, oportuno, relevante y no excesivo en relación con dicha finalidad o con la naturaleza de los datos.

A este núcleo se añaden el principio de confidencialidad (literal g), que impone reserva sobre los datos tratados; el de calidad y exactitud (literal h), que obliga a mantener la información veraz, completa y actualizada; el de conservación (literal i), que limita el tiempo durante el cual los datos pueden mantenerse almacenados; el de seguridad de datos personales (literal j), que exige adoptar medidas técnicas y organizativas para proteger la información frente a accesos no autorizados, pérdidas o alteraciones; y el de responsabilidad proactiva y demostrada (literal k), conforme al cual el responsable del tratamiento debe estar en condiciones de probar en todo momento el cumplimiento de sus obligaciones (Asamblea Nacional del Ecuador, 2021). La enumeración de principios concluye con el de aplicación favorable al titular (literal l), que ordena resolver cualquier duda sobre el alcance de sus derechos en el sentido más beneficioso para la persona cuyos datos son objeto de tratamiento, y con el de independencia del control (literal m), que exige que la Autoridad de Protección de Datos ejerza sus funciones de forma independiente, imparcial y autónoma, llevando a cabo las respectivas acciones de prevención, investigación y sanción.

Naranjo Godoy (2017) sostiene que estos principios constituyen auténticas garantías jurídicas orientadas a que toda actuación relacionada con la información de una persona respete sus derechos fundamentales; no son, por tanto, directrices administrativas de cumplimiento

discrecional, sino criterios jurídicos obligatorios para quien trate datos personales. En la misma dirección, Herrán Ortiz (2003) advierte que un sistema de protección de datos que enuncie principios sin dotarlos de mecanismos de exigibilidad corre el riesgo de convertirse en una fórmula retórica, incapaz de modificar las prácticas reales de quienes manejan la información.

Junto con estos principios, la legislación ecuatoriana reconoce un conjunto de derechos que permiten al titular ejercer un control efectivo sobre su información. Se trata, en esencia, de una versión ampliada de los clásicos derechos ARCO (acceso, rectificación, cancelación y oposición) que la doctrina latinoamericana ha empleado tradicionalmente para sintetizar el contenido subjetivo de esta materia: el derecho de acceso (artículo 13), que permite conocer qué datos están siendo tratados y con qué finalidad; el de rectificación y actualización (artículo 14), que faculta corregir información inexacta o incompleta; el de supresión o eliminación (artículo 15) término que la LOPDP prefiere al de "cancelación", que permite solicitar que los datos dejen de tratarse cuando ya no sean necesarios o su tratamiento resulte improcedente; y el de oposición (artículo 16), que faculta rechazar determinados tratamientos cuando concurren los motivos legítimos previstos por la ley.

A ellos se suma el derecho a la portabilidad (artículo 17), que faculta obtener la información personal en un formato estructurado para transmitirla a otro responsable; el derecho a la suspensión del tratamiento (artículo 19), que permite congelar temporalmente determinadas operaciones sobre los datos mientras se resuelve una controversia sobre su licitud; y el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas (artículo 20), garantía que cobra particular importancia frente al uso creciente de algoritmos de calificación crediticia, perfilamiento comercial o selección de personal, y que busca asegurar que

ninguna persona sea sometida a decisiones con efectos jurídicos significativos sin la posibilidad de intervención humana.

Estos derechos constituyen la manifestación práctica del principio de autodeterminación informativa, en la medida en que permiten al titular participar activamente en las decisiones relacionadas con su información y exigir el respeto de las garantías previstas por el ordenamiento jurídico. Como señala Pérez Luño (2012), el reconocimiento de facultades de control sobre los datos personales responde a la necesidad de fortalecer la posición de la persona frente a los riesgos que genera la sociedad de la información. Ahora bien, la sola enunciación legal de estos derechos no garantiza su ejercicio: su eficacia depende de que existan procedimientos claros, plazos razonables y una autoridad con capacidad real para atender los reclamos de los titulares, aspecto cuya verificación práctica corresponde precisamente al análisis institucional que se desarrolla más adelante en este trabajo.

Los principios y derechos previstos en la LOPDP constituyen, en suma, las herramientas jurídicas mediante las cuales el titular puede exigir un tratamiento de su información conforme a los estándares legales. Sin embargo, la eficacia de estas garantías depende de la existencia de un marco institucional capaz de asegurar su cumplimiento. Corresponde, en consecuencia, examinar la regulación jurídica de la protección de datos personales en el Ecuador y la forma en que el ordenamiento desarrolla estas garantías constitucionales y legales.

2.3. Regulación jurídica de la protección de datos personales en el Ecuador

La regulación jurídica de la protección de los datos personales en el Ecuador es el resultado de un proceso de evolución constitucional y legislativa orientado a garantizar el control que toda persona ejerce sobre la información que la identifica. El desarrollo acelerado de las tecnologías de la información, la expansión de los servicios digitales y el tratamiento masivo de

datos personales evidenciaron la necesidad de establecer un marco jurídico que reconociera y desarrollara la protección de los datos personales como un derecho fundamental autónomo, dotado de principios, garantías e instituciones encargadas de asegurar su ejercicio efectivo.

Esta regulación se remonta a la reforma constitucional de 1996, mediante la cual se incorporó la garantía jurisdiccional del hábeas data como mecanismo destinado a permitir que las personas conocieran, accedieran y solicitaran la rectificación de la información personal contenida en archivos o bases de datos administradas por entidades públicas y privadas. Como explica Naranjo Godoy (2017), esta incorporación representó un antecedente relevante en el reconocimiento jurídico de la necesidad de proteger la información personal; sin embargo, dicha protección permanecía estrechamente vinculada al derecho a la intimidad y todavía no existía un reconocimiento expreso del derecho a la protección de datos personales como una categoría jurídica independiente.

El cambio más significativo se produjo con la entrada en vigencia de la Constitución de la República del Ecuador de 2008, cuyo artículo 66, numeral 19, reconoció expresamente el derecho a la protección de datos personales como un derecho fundamental autónomo. Esta disposición establece que toda persona tiene derecho al acceso y a la decisión sobre la información y los datos de carácter personal, así como a su correspondiente protección, disponiendo además que la recolección, almacenamiento, procesamiento, distribución o difusión de dichos datos requiere la autorización de su titular o mandato expreso de la ley (Asamblea Nacional del Ecuador, 2008). Según Naranjo Godoy (2017), este reconocimiento constitucional incorpora el principio de autodeterminación informativa, entendido como la facultad que tiene toda persona para controlar la obtención, utilización, almacenamiento, circulación y tratamiento

de la información que la identifica. Bajo esta perspectiva, los datos personales dejan de ser únicamente una manifestación del derecho a la intimidad y adquieren autonomía como bien jurídico digno de protección constitucional.

El reconocimiento constitucional por sí solo no resultó suficiente para garantizar plenamente este derecho. Enríquez Álvarez (2017) sostiene que la Constitución de 2008 reconoció la protección de datos personales sin desarrollar una definición jurídica precisa del concepto de dato personal ni establecer reglas específicas sobre su tratamiento, conservación, circulación o transferencia. Asimismo, el texto constitucional tampoco determinó principios técnicos ni obligaciones concretas para las entidades públicas y privadas responsables del tratamiento de información, circunstancia que generó importantes vacíos normativos y evidenció la necesidad de una legislación especializada que desarrollara el contenido y alcance del derecho constitucionalmente reconocido.

Adquiere especial importancia la garantía jurisdiccional del hábeas data, prevista en el artículo 92 de la Constitución, cuyo objeto consiste en proteger la información personal contenida en documentos, archivos, registros o bases de datos administradas tanto por entidades públicas como privadas. Según Naranjo Godoy (2017), esta garantía constituye el principal mecanismo constitucional de tutela del derecho a la protección de datos personales, al permitir que el titular conozca la información existente sobre su persona, solicite su actualización, rectificación, eliminación u oposición frente a tratamientos que vulneren sus derechos. De esta manera, el hábeas data representa el puente entre el reconocimiento constitucional del derecho y su protección efectiva frente a actuaciones arbitrarias o ilegítimas.

Desde la perspectiva del constitucionalismo ecuatoriano, Ávila Santamaría (2008) sostiene que el Estado constitucional de derechos y justicia no puede limitarse al reconocimiento formal de los derechos fundamentales, sino que debe garantizar su eficacia mediante instituciones, procedimientos y mecanismos capaces de hacerlos exigibles en la práctica. Bajo esta concepción, la protección de los datos personales exige no solo la proclamación constitucional del derecho, sino también la existencia de instrumentos normativos e institucionales que permitan prevenir su vulneración, reparar los daños ocasionados y asegurar que las personas ejerzan un control real sobre la información que las identifica. Esta visión adquiere especial relevancia frente al crecimiento de las tecnologías digitales y al incremento de los delitos informáticos, cuya complejidad demanda respuestas jurídicas coordinadas entre el derecho constitucional, el derecho administrativo y el derecho penal.

En desarrollo de este mandato constitucional, el fundamento jurídico de la protección de datos personales se consolidó con la expedición de la Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Registro Oficial Suplemento N.º 459 de 26 de mayo de 2021, que se convirtió en el principal instrumento normativo de la materia al regular los principios del tratamiento de datos, los derechos de los titulares, las obligaciones de responsables y encargados, así como los mecanismos administrativos de cumplimiento. Resulta significativo que entre el reconocimiento constitucional del derecho en 2008 y la expedición de la LOPDP transcurrieran trece años, circunstancia que evidencia que el Ecuador reconoció tempranamente este derecho, pero demoró considerablemente en dotarlo de un desarrollo legislativo que permitiera su aplicación efectiva.

La ley previó un régimen de adecuación progresiva mediante sus disposiciones transitorias, otorgando a las entidades públicas y privadas un plazo de hasta dos años para adaptar sus procesos de tratamiento de datos a las nuevas exigencias legales, por lo que gran parte de sus disposiciones adquirieron plena exigibilidad durante el año 2023.

Uno de los aportes más relevantes de la LOPDP fue la creación de la Superintendencia de Protección de Datos Personales (SPDP), definida por el artículo 76 de la ley como el órgano de control y vigilancia encargado de garantizar a la ciudadanía la protección de sus datos personales. La SPDP cuenta con potestad sancionatoria, personalidad jurídica y autonomía administrativa, técnica, operativa y financiera, y ejerce sus funciones a través de una estructura desconcentrada que incluye intendencias especializadas.

En ejercicio de su facultad normativa, la Superintendencia de Protección de Datos Personales SPDP ha expedido normativa secundaria en distintas materias, entre ellas la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial Resolución SPDP-SPD-2026-0009-R, que establece disposiciones específicas aplicables al tratamiento de datos personales en sistemas de inteligencia artificial y la Norma General de Transferencias de datos personales, mediante la Resolución SPDP-SPD-2026-0004-R. Asimismo, la SPDP ha implementado un mecanismo de atención de denuncias ciudadanas por incumplimiento de la LOPDP, mediante el cual puede iniciar actuaciones previas, imponer medidas provisionales de protección o dar inicio a un proceso administrativo sancionador (Superintendencia de Protección de Datos Personales, 2026).

La legislación ecuatoriana impone, además, obligaciones específicas a los responsables y encargados del tratamiento de datos personales, entre ellas, la observancia de los principios

previstos en la LOPDP, la implementación de medidas técnicas y organizativas de seguridad, la preservación de la confidencialidad de la información y el cumplimiento del principio de responsabilidad proactiva y demostrada. No obstante, la aplicación práctica de estas obligaciones podría plantear desafíos en sectores particularmente sensibles, como el financiero, sanitario y de telecomunicaciones, especialmente cuando no existen estándares técnicos específicos que orienten su implementación de acuerdo con las particularidades de cada sector. Esta situación podría incrementar los riesgos para los titulares de los datos y dificultar la adopción de medidas adecuadas para garantizar una protección efectiva de su información personal.

En el ámbito comparado, la LOPDP evidencia una marcada influencia del Reglamento General de Protección de Datos de la Unión Europea (RGPD) al incorporar principios como la licitud, transparencia, finalidad, minimización, seguridad y responsabilidad proactiva, así como derechos equivalentes de acceso, rectificación, supresión, oposición y portabilidad. Sin embargo, mientras el modelo europeo cuenta con una consolidada experiencia institucional y jurisprudencial, el sistema ecuatoriano aún se encuentra en una etapa de fortalecimiento. De igual forma, experiencias latinoamericanas como las de Argentina, Colombia y Chile demuestran que la eficacia de un régimen de protección de datos depende no únicamente de la existencia de una ley especializada, sino también de la capacidad técnica, institucional y presupuestaria de la autoridad encargada de garantizar su cumplimiento.

En definitiva, el ordenamiento jurídico ecuatoriano cuenta actualmente con un marco constitucional y legal que reconoce el derecho a la protección de los datos personales, regula su tratamiento e impone obligaciones a quienes intervienen en el manejo de la información. No obstante, el acelerado desarrollo de las tecnologías digitales y el incremento de las amenazas

derivadas de los delitos informáticos evidencian que la eficacia de este sistema no depende exclusivamente de la existencia de normas jurídicas, sino también de la adecuada articulación entre la Constitución, la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal. Precisamente, el análisis de esa articulación permitirá determinar si el marco jurídico vigente ofrece una tutela efectiva frente a las nuevas formas de vulneración de los datos personales o si persisten limitaciones que justifican la necesidad de fortalecer la protección constitucional de este derecho fundamental.

2.4. Protección de los datos personales frente a los delitos informáticos

La acelerada transformación digital ha multiplicado la generación, el almacenamiento y la circulación de datos personales a través de plataformas tecnológicas, redes sociales, servicios financieros electrónicos y sistemas de información públicos y privados. Estos avances han facilitado, sin duda, el acceso a bienes y servicios; pero también han incrementado los riesgos asociados al tratamiento indebido de la información, al punto de convertir a los datos personales en uno de los principales objetivos de la delincuencia informática contemporánea.

Los delitos informáticos, también llamados ciberdelitos, comprenden aquellas conductas ilícitas que utilizan las tecnologías de la información como medio, instrumento o finalidad para vulnerar bienes jurídicos protegidos. El surgimiento de estas tecnologías no creó simplemente nuevas formas de cometer los delitos de siempre, sino que transformó la criminalidad en su conjunto: así lo plantea Miró Llinares (2012), quien ubica en el desarrollo del ciberespacio el origen de modalidades delictivas capaces de afectar tanto el patrimonio como la intimidad y otros bienes jurídicos que antes no se veían comprometidos por este tipo de conductas.

Esta transformación trae consigo un problema adicional, que Acurio Del Pino (2015) desarrolla con particular claridad para el contexto ecuatoriano: la mayoría de los delitos informáticos no lesionan un solo bien jurídico, sino varios a la vez. El autor lo llama carácter pluriofensivo, y lo ilustra con un ejemplo sencillo pero elocuente: cuando alguien vulnera un sistema informático para acceder a información personal, no solo se está atacando la intimidad de la víctima, sino también la confianza colectiva depositada en la seguridad de los sistemas informáticos. Ambas afectaciones ocurren de manera simultánea, no sucesiva ni separable.

Esta característica tiene consecuencias prácticas importantes para el presente estudio. Si un mismo hecho puede lesionar al mismo tiempo la protección de datos personales y otros bienes jurídicos el patrimonio, la seguridad informática, la fe pública, entonces determinar con precisión qué norma resulta aplicable, o si el marco jurídico vigente cubre adecuadamente todas las dimensiones afectadas, deja de ser un ejercicio sencillo de subsunción y se convierte en un problema interpretativo real. Es precisamente esta complejidad la que justifica examinar si la articulación actual entre la Constitución, la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal resulta suficiente para responder a conductas que, por su propia naturaleza, rara vez afectan un único interés jurídico.

Esa precisión resulta indispensable para delimitar el objeto de la presente investigación. El Código Orgánico Integral Penal (COIP) tipifica, en su sección de delitos contra la seguridad de los activos de los sistemas de información y comunicación, conductas como la revelación ilegal de base de datos (artículo 229), la interceptación ilegal de datos (artículo 230) y el acceso no consentido a un sistema informático, telemático o de telecomunicaciones (artículo 234); a

ellas se suma, en el título de los delitos contra el derecho a la intimidad, la violación a la intimidad prevista en el artículo 178.

No todas estas figuras protegen el mismo interés jurídico ni con la misma intensidad. Los artículos 178 y 229 recaen de manera directa sobre la intimidad y la información personal, porque ambos tipifican expresamente la afectación al secreto, la intimidad o la privacidad de las personas. El artículo 234, en cambio, protege primordialmente la seguridad e integridad del sistema informático frente al acceso no autorizado, y solo incide sobre la protección de datos personales cuando el sistema vulnerado efectivamente almacena o procesa información de esa naturaleza: no todo acceso no consentido implica, por sí solo, una vulneración de datos personales.

El artículo 230 del COIP requiere una precisión por su relación directa con el phishing. En su numeral 1 se sanciona la interceptación de datos, mientras que el numeral 2 contempla conductas que se relacionan directamente con esta modalidad, como el diseño o envío de páginas, enlaces o ventanas emergentes engañosas, así como la modificación de la resolución de nombres de dominio con la finalidad de inducir a una persona a ingresar a un sitio diferente al que pretendía acceder. Esta conducta constituye uno de los elementos centrales del phishing, ya que busca engañar a la víctima para obtener información o dirigirla hacia un sitio controlado por el autor. Por su parte, el numeral 4 contempla la clonación o comercialización de información contenida en tarjetas de pago, conducta que también puede estar vinculada con este tipo de fraude.

Por ello, aunque el ordenamiento jurídico ecuatoriano no contempla un delito denominado expresamente “phishing”, esta conducta no queda sin respuesta penal. El artículo

230, numeral 2, permite sancionar determinadas acciones que forman parte de esta modalidad, especialmente aquellas relacionadas con el engaño utilizado para dirigir a la víctima hacia sitios o enlaces falsos. Además, cuando como consecuencia de este engaño se produce un perjuicio económico, los hechos podrían también ser analizados bajo el delito de apropiación fraudulenta por medios electrónicos, previsto en el artículo 190 del COIP. En consecuencia, la calificación jurídica dependerá de las circunstancias concretas del caso y de si se analiza principalmente el mecanismo de engaño empleado o el perjuicio patrimonial ocasionado.

Por esta razón, la presente investigación centra su análisis principalmente en los artículos 178, 229 y 230 del COIP, debido a que las conductas contempladas en estas normas tienen una relación más directa con la afectación del derecho a la protección de datos personales. El artículo 234 se considera únicamente cuando el acceso no consentido se produce sobre sistemas que contienen información personal, mientras que el artículo 190 se aborda como una referencia complementaria para analizar la posible afectación patrimonial derivada del phishing, sin que constituya uno de los ejes centrales de esta investigación.

La suplantación de identidad requiere, por su parte, una consideración particular, ya que no toda conducta de este tipo implica necesariamente una vulneración del derecho a la protección de datos personales. El artículo 212 del COIP reconoce la suplantación de identidad como un delito autónomo dentro de los delitos contra el derecho a la identidad y no dentro de aquellos relacionados directamente con la protección de la información personal. La norma sanciona a quien, de cualquier manera, suplante la identidad de otra persona con la finalidad de obtener un beneficio para sí mismo o para un tercero, causando un perjuicio a la víctima. Por tanto, para que esta conducta se configure debe existir un beneficio como parte de sus elementos, sin que el

artículo establezca expresamente que la suplantación deba realizarse mediante medios físicos o digitales.

La relación entre la suplantación de identidad y la protección de datos personales aparece cuando, para hacerse pasar por otra persona, se obtienen, utilizan o tratan de manera ilícita sus datos personales. Esto puede suceder, por ejemplo, cuando una persona accede sin autorización a las credenciales, fotografías, datos biométricos o información de contacto de una víctima y posteriormente utiliza esos datos para hacerse pasar por ella en un entorno digital. Dependiendo de las circunstancias, estas acciones podrían también relacionarse con los delitos previstos en los artículos 229, sobre revelación ilegal de base de datos, o 234, relacionado con el acceso no consentido a un sistema informático. Un ejemplo de ello sería la creación de perfiles falsos en redes sociales o la apertura de cuentas y líneas de servicio utilizando los datos de otra persona.

En estos casos, la suplantación de identidad y la vulneración de datos personales no constituyen necesariamente una misma conducta. La vulneración de los datos puede ser el medio utilizado para hacer posible posteriormente la suplantación. Esta diferencia es importante porque permite determinar con mayor claridad qué derecho está siendo afectado y qué normas pueden resultar aplicables dependiendo de las circunstancias del caso.

Por el contrario, existen situaciones en las que una persona puede suplantar a otra sin que necesariamente exista un tratamiento previo de sus datos personales. Esto podría ocurrir, por ejemplo, mediante la simple utilización verbal del nombre de otra persona o mediante determinadas formas de falsificación de documentos que no impliquen el acceso o uso de información personal digitalizada. En estos casos, podría aplicarse el artículo 212 del COIP sin que exista necesariamente una vulneración del derecho a la protección de datos personales.

Esta distinción resulta relevante para la presente investigación, ya que permite establecer con mayor precisión cuándo la suplantación de identidad forma parte del objeto de estudio, por estar relacionada con el tratamiento ilícito de datos personales, y cuándo corresponde principalmente al ámbito de protección del derecho a la identidad. Además, la exigencia de que exista un beneficio para el autor o para un tercero puede generar ciertas dificultades frente a algunas formas de suplantación que se presentan en entornos digitales. Por ejemplo, la creación de perfiles falsos con fines de acoso, humillación o desprestigio, sin que exista un beneficio económico o de otra naturaleza para quien realiza la conducta, podría no encajar de manera clara en el alcance del artículo 212. Esto evidencia la necesidad de analizar las características particulares de las conductas digitales y su relación con la protección de los datos personales, especialmente cuando el uso indebido de esta información puede generar un perjuicio a la víctima aun cuando no exista un beneficio directo para el responsable.

Como plantea Pérez Luño (2012), en su análisis de los derechos humanos frente a la sociedad tecnológica, el desarrollo de las nuevas tecnologías exige que la protección de los derechos fundamentales no se limite al reconocimiento formal de garantías jurídicas, sino que responda de manera efectiva a los riesgos que ese desarrollo genera. La protección de los datos personales no puede entenderse, entonces, como una obligación meramente administrativa: constituye, ante todo, un mecanismo de prevención cuyo fracaso abre la puerta a la intervención penal, y cuya eficacia debe medirse, en consecuencia, tanto por su capacidad de evitar la vulneración como por la respuesta que el sistema de justicia ofrece cuando esa vulneración ya se produjo.

En el caso ecuatoriano, el incremento del uso de medios electrónicos en las actividades comerciales, financieras y administrativas ha ampliado las posibilidades de tratamiento y con ellas, de vulneración de los datos personales. La experiencia práctica revela además, una dificultad adicional que la sola lectura de las normas no evidencia: la investigación de los delitos informáticos delimitados exige capacidades técnicas especializadas, como el peritaje informático forense, la cooperación con proveedores de servicios digitales y la preservación de evidencia volátil que no siempre están disponibles con la misma celeridad con que se comete la conducta delictiva, de modo que la eficacia del sistema jurídico no depende únicamente de la existencia de los tipos penales, sino de la capacidad institucional para investigarlos y sancionarlos oportunamente.

La estrecha relación entre los delitos informáticos así delimitados y la protección de los datos personales evidencia que las amenazas del entorno digital trascienden lo tecnológico y generan consecuencias jurídicas relevantes para personas e instituciones. El estudio de estas conductas no solo permite comprender las formas en que pueden vulnerarse los datos personales, sino que plantea la necesidad de evaluar si las garantías del ordenamiento jurídico ecuatoriano tanto la vía preventiva de la LOPDP como la vía represiva del COIP resultan suficientes frente a estos riesgos. Esa evaluación es, precisamente, el objeto del análisis de eficacia que se desarrolla a continuación.

Si bien los delitos informáticos comprenden un conjunto amplio de conductas ilícitas cometidas mediante el uso de las tecnologías de la información, no todas ellas afectan de manera directa el derecho a la protección de datos personales. En este sentido, la presente investigación delimita su objeto de estudio al análisis de aquellas conductas que implican el acceso, tratamiento, utilización o divulgación ilícita de datos personales, por ser las que guardan una

relación inmediata con el derecho reconocido en el artículo 66, numeral 19, de la Constitución de la República del Ecuador (Asamblea Constituyente del Ecuador, 2008) y desarrollado por la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021). Esta delimitación permite mantener coherencia entre el problema jurídico, los objetivos y el desarrollo de la investigación.

2.5. Eficacia de la protección jurídica frente a los delitos informáticos

Para efectos de esta investigación, la eficacia de la protección jurídica de los datos personales se entenderá como la capacidad del ordenamiento para garantizar, de forma articulada, ocho dimensiones: (i) la prevención de vulneraciones mediante el régimen de principios y obligaciones de la LOPDP; (ii) la protección activa del titular durante el tratamiento; (iii) la existencia de mecanismos de tutela administrativa y jurisdiccional accesibles; (iv) la capacidad de investigación de las conductas que constituyen delito; (v) la efectiva sanción de los responsables; (vi) la reparación del daño ocasionado al titular; (vii) la capacidad institucional técnica y presupuestaria de los organismos competentes; y (viii) la articulación entre dichas autoridades. Un sistema jurídico que reconozca el derecho, pero falle en alguna de estas dimensiones no puede considerarse plenamente eficaz, aun cuando cuente con normas vigentes. En esta investigación, estas dimensiones constituyen los criterios de análisis utilizados para determinar si el marco jurídico ecuatoriano ofrece una protección efectiva de los datos personales frente a los delitos informáticos

La protección de los datos personales no se agota en su reconocimiento como derecho fundamental en la Constitución, ni en la expedición de una legislación especializada. La verdadera garantía de este derecho depende de su eficacia, entendida como la capacidad del ordenamiento jurídico para prevenir vulneraciones, proteger a los titulares y ofrecer mecanismos idóneos para restablecer sus derechos cuando han sido afectados. La eficacia jurídica supone, en consecuencia, evaluar no solo la existencia de normas, sino también su aplicación práctica y la capacidad real de las instituciones para hacerlas cumplir. Desde la perspectiva garantista, Ferrajoli (2006) sostiene que un derecho fundamental solo puede considerarse efectivo cuando el ordenamiento jurídico establece garantías que aseguren su cumplimiento y mecanismos idóneos para reaccionar frente a su vulneración. El reconocimiento constitucional de un derecho resulta insuficiente, advierte, si no viene acompañado de instrumentos jurídicos e institucionales que lo hagan exigible y lo protejan de manera efectiva. Alexy (2007), por su parte, entiende los derechos fundamentales como principios que deben realizarse en la mayor medida posible dentro de las posibilidades jurídicas y fácticas existentes; desde esa óptica, la protección de los datos personales exige del Estado no solo la promulgación de normas, sino también políticas públicas, mecanismos administrativos y herramientas judiciales que garanticen su aplicación efectiva frente a los riesgos derivados del tratamiento indebido de la información y de los delitos informáticos.

En el ámbito de la sociedad digital, Pérez Luño (2012) señala que el desarrollo de las tecnologías de la información transformó profundamente las formas de ejercer y proteger los derechos fundamentales: el intercambio constante de información, la automatización de procesos y la utilización masiva de datos personales incrementaron las posibilidades de vulneración de la

privacidad, obligando al Derecho a evolucionar mediante mecanismos de protección genuinamente eficaces. Ávila Santamaría (2008) añade, desde la dogmática constitucional ecuatoriana, que el reconocimiento del derecho a la protección de datos personales representa un avance significativo dentro del Estado constitucional de derechos y justicia proclamado por el artículo 1 de la Constitución; sin embargo, advierte que la eficacia de cualquier derecho reconocido bajo ese modelo depende de que existan mecanismos institucionales que garanticen su control efectivo, pues un Estado constitucional de derechos que se limita a enunciarlos sin materializarlos termina reproduciendo la misma distancia entre norma y realidad que ese modelo pretendía superar.

2.5.1 Derecho comparado: experiencias de España, Colombia, Argentina y Chile

El análisis del derecho comparado permite identificar experiencias que pueden contribuir a evaluar las fortalezas y limitaciones del sistema ecuatoriano en materia de protección de datos personales. Para ello, resulta pertinente considerar los modelos desarrollados en España, Colombia, Argentina y Chile, seleccionados por representar distintos niveles de madurez institucional frente a un mismo problema: la tutela efectiva de los datos personales frente a su uso indebido.

En España, la regulación aplicable combina el Reglamento General de Protección de Datos de la Unión Europea (RGPD) con la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD). La autoridad competente es la Agencia Española de Protección de Datos (AEPD), un organismo administrativo independiente creado en 1992 y reorganizado por la LOPDGDD, que ejerce funciones de investigación de

oficio o por denuncia, auditorías preventivas sectoriales y potestad sancionadora, con multas que pueden alcanzar los 20 millones de euros o el 4% de la facturación global de la empresa infractora. El aspecto más relevante que puede tomarse como referencia para el caso ecuatoriano es la capacidad de la autoridad española para actuar de manera preventiva, sin depender exclusivamente de la denuncia presentada por el titular de los datos. Esto le permite iniciar investigaciones y realizar auditorías de oficio en determinados sectores cuando existen razones que justifican su intervención. Esta forma de actuación proactiva representa una diferencia importante frente al modelo ecuatoriano, cuya actuación ha sido principalmente reactiva. Por ello, este referente comparado constituye la base para plantear el fortalecimiento de las facultades de investigación y auditoría de oficio de la Superintendencia de Protección de Datos Personales, propuesta que se desarrolla más adelante en esta investigación.

En Colombia, la regulación aplicable es la Ley 1581 de 2012, desarrollada por el Decreto 1377 de 2013 y complementada, en materia de datos financieros, por la Ley 1266 de 2008. La autoridad competente es la Superintendencia de Industria y Comercio (SIC), a través de su Delegatura para la Protección de Datos Personales, con facultades de vigilancia, investigación de oficio o a petición de parte, y potestad sancionadora graduada conforme a criterios legales expresos (artículo 24 de la ley). Un mecanismo particular es el Registro Nacional de Bases de Datos, de consulta pública, que exige a los responsables reportar sus políticas de tratamiento.

Resulta relevante señalar que el régimen colombiano contempla sanciones de hasta 10.000 salarios mínimos o el 5% de los ingresos operacionales del infractor, lo que evidencia que incluso un sistema más antiguo que el ecuatoriano cuenta con mecanismos sancionadores frente a los riesgos actuales. El aspecto que resulta especialmente relevante para el contexto ecuatoriano es la existencia de un registro público de bases de datos, ya que este mecanismo

puede contribuir a mejorar la transparencia y permitir un mayor seguimiento sobre el tratamiento de la información personal. En esta investigación, esta herramienta se plantea como un elemento complementario de la propuesta jurídica, debido a que podría proporcionar información útil para fortalecer la coordinación entre las instituciones involucradas y facilitar la identificación de responsables del tratamiento de datos que puedan representar un mayor nivel de riesgo.

En Argentina, la Ley 25.326, vigente desde el año 2000, constituye el marco principal, reglamentada por el Decreto 1558/2001. Desde 2017, la autoridad de aplicación es la Agencia de Acceso a la Información Pública (AAIP), un ente autárquico con autonomía funcional que puede dictar normativa técnica e imponer sanciones administrativas (apercibimiento, suspensión, multa o cancelación del registro). Este es un caso particularmente ilustrativo para Ecuador porque evidencia que la existencia de una regulación específica no garantiza por sí misma una protección efectiva frente a los riesgos del entorno digital. El caso analizado permite extraer una enseñanza importante para el contexto ecuatoriano: contar con una legislación que reconozca y proteja los datos personales constituye un avance significativo, pero no es suficiente si las normas y el régimen sancionador no se mantienen actualizados frente a los cambios tecnológicos y a las nuevas formas de vulneración. Esta experiencia evidencia la necesidad de revisar periódicamente la normativa para evitar que pierda eficacia con el paso del tiempo. Por ello, esta consideración sirve de fundamento para plantear, dentro de la propuesta jurídica, una cláusula de revisión periódica del régimen sancionador.

En Chile, la Ley 21.719, publicada el 13 de diciembre de 2024, reforma íntegramente el régimen anterior (Ley 19.628 de 1999) y crea la Agencia de Protección de Datos Personales (APDP), dotada de facultades de fiscalización, investigación de oficio y sanción. Debe precisarse

que la Ley 21.719 tiene prevista su entrada en plena vigencia para el 1 de diciembre de 2026. Hasta esa fecha, el régimen anterior establecido por la Ley 19.628 continúa siendo aplicable, mientras el nuevo marco normativo se encuentra en proceso de implementación. El análisis del caso chileno resulta relevante para Ecuador desde dos aspectos. En primer lugar, el paso de un modelo en el que no existía una autoridad de control con competencias sancionadoras plenamente desarrolladas hacia un sistema con una institución especializada guarda cierta relación con el proceso ecuatoriano, que pasó del reconocimiento constitucional del derecho en 2008 a la expedición de la LOPDP en 2021. En segundo lugar, la posibilidad de que la autoridad chilena realice investigaciones de oficio, sin depender únicamente de una denuncia o solicitud de parte, constituye un referente importante para Ecuador. Junto con la experiencia española, este modelo comparado fortalece la propuesta de otorgar a la Superintendencia de Protección de Datos Personales mayores facultades para realizar investigaciones de oficio, como parte de las medidas planteadas en esta investigación.

De manera comparativa, las cuatro experiencias permiten advertir que la protección efectiva de los datos personales no depende únicamente de contar con una ley que reconozca el derecho, sino de tres factores adicionales: una autoridad con capacidad de actuación proactiva (España), mecanismos de transparencia y trazabilidad institucional (Colombia), y un régimen sancionador que se actualice al ritmo de los riesgos tecnológicos (la lección, en sentido negativo, de Argentina). Chile, por su parte, ofrece el paralelo más cercano al propio proceso de maduración institucional que atraviesa Ecuador. En conjunto, el análisis comparado de los casos estudiados permite sustentar las diferentes propuestas planteadas en esta investigación. Las experiencias de España y Chile sirven como referentes para fortalecer la facultad de investigación de oficio de la Superintendencia de Protección de Datos Personales, mientras que

los modelos de Colombia y Argentina aportan elementos útiles para plantear la implementación de un registro público y la revisión periódica del régimen sancionador. Por su parte, la propuesta de coordinación interinstitucional entre las autoridades ecuatorianas surge directamente de las dificultades identificadas en el análisis institucional, especialmente en relación con la falta de articulación entre las entidades encargadas de prevenir, investigar y sancionar las conductas que afectan los datos personales.

2.5.2 Eficacia institucional en la protección de los datos personales

La protección efectiva de los datos personales no depende únicamente de la existencia de normas constitucionales y legales, sino también de la capacidad de las instituciones encargadas de prevenir, investigar y sancionar las conductas que pueden vulnerar este derecho. En Ecuador, esta protección requiere la intervención coordinada de las autoridades responsables del control de datos personales, la investigación penal y la administración de justicia.

La Superintendencia de Protección de Datos Personales cumple un papel fundamental en la supervisión del cumplimiento de las obligaciones relacionadas con el tratamiento de datos personales, mientras que la Fiscalía General del Estado interviene cuando los hechos pueden constituir una infracción penal, desarrollando las investigaciones correspondientes. A estas instituciones se suman la Policía Nacional y los órganos jurisdiccionales, cuya actuación resulta necesaria para la investigación, obtención y valoración de la evidencia y la determinación de las responsabilidades correspondientes.

Sin embargo, la eficacia de esta protección podría verse limitada por posibles desafíos de coordinación entre las instituciones, por una eventual insuficiencia de especialización técnica, o

por dificultades en la investigación de conductas cometidas mediante medios digitales, factores que esta investigación busca precisamente contrastar con la evidencia disponible, sin presuponerlos como hechos ya comprobados.

Por ello, la existencia de instituciones con competencias específicas constituye un avance importante, aunque no garantiza por sí sola una tutela efectiva si los desafíos señalados llegaran a confirmarse. En la medida en que el análisis desarrollado a continuación así lo evidencie, sería pertinente fortalecer la coordinación entre las autoridades administrativas y penales, así como sus capacidades técnicas y mecanismos de actuación, de manera que la protección reconocida constitucionalmente pueda traducirse en una respuesta efectiva frente a las vulneraciones de datos personales.

2.5.3 Análisis crítico de la protección jurídica de los datos personales frente a los delitos informáticos

A partir de las ocho dimensiones de eficacia establecidas para esta investigación, el análisis realizado permite valorar de manera diferenciada cómo funciona el sistema jurídico ecuatoriano frente a la protección de los datos personales relacionados con los delitos informáticos.

En materia de prevención, la Ley Orgánica de Protección de Datos Personales establece principios, obligaciones y responsabilidades dirigidas a quienes realizan el tratamiento de datos personales. Este marco constituye una base importante para prevenir posibles vulneraciones. Sin embargo, el análisis comparado con el modelo español permitió advertir que la ausencia de una facultad claramente desarrollada para que la Superintendencia de Protección de Datos Personales

realice investigaciones y auditorías de oficio limita su capacidad para detectar y corregir posibles riesgos antes de que estos lleguen a convertirse en vulneraciones. Por ello, aunque la prevención se encuentra reconocida en el ámbito normativo, todavía presenta ciertas limitaciones en su aplicación práctica.

Respecto de la protección activa del titular, los derechos reconocidos en los artículos 14 al 21 de la LOPDP, entre ellos los derechos de rectificación, supresión, oposición y portabilidad, representan un desarrollo jurídico amplio y acorde con los estándares observados en otros ordenamientos. En este sentido, puede considerarse que existe una protección formal adecuada del titular, pues la legislación le proporciona herramientas para ejercer control sobre sus datos personales y exigir que estos sean tratados conforme a la ley.

En cuanto a la tutela administrativa y jurisdiccional, el análisis de la jurisprudencia de la Corte Constitucional demuestra que existe un desarrollo importante respecto de la naturaleza, contenido y alcance de la garantía de hábeas data. La Corte ha contribuido a precisar el alcance de esta garantía y su relación con la protección de los datos personales. Sin embargo, el caso resuelto mediante la Sentencia 182-15-SEP-CC también permite observar que, a pesar de contar con una garantía constitucional reconocida, existieron dificultades relacionadas con su aplicación procesal, particularmente respecto del plazo para su activación, situación que tuvo que ser aclarada mediante interpretación jurisprudencial. Esto evidencia que la tutela jurisdiccional presenta un desarrollo importante en el ámbito doctrinal, pero todavía puede enfrentar dificultades prácticas que afectan la oportunidad de la protección.

Sobre la capacidad de investigación, el análisis normativo e institucional permitió identificar que la investigación de los delitos informáticos relacionados con la vulneración de

datos personales requiere conocimientos y recursos técnicos especializados. Entre ellos se encuentran el peritaje informático forense, la preservación de evidencia digital y la cooperación con proveedores de servicios tecnológicos. Estas necesidades pueden representar una dificultad cuando no existe una respuesta técnica suficientemente oportuna. No obstante, es importante señalar que esta investigación no dispone de información estadística propia que permita determinar con precisión el alcance de esta problemática. Por ello, más que afirmar la existencia de una deficiencia generalizada, se la considera una limitación identificada a partir del análisis jurídico e institucional y, al mismo tiempo, una de las áreas que requiere mayor estudio empírico.

En materia de sanción efectiva, la Superintendencia de Protección de Datos Personales cuenta con potestades sancionadoras establecidas en la LOPDP y ha avanzado en la emisión de normativa secundaria para desarrollar sus competencias (SPDP, 2026). Sin embargo, debido a que se trata de una institución de reciente creación, todavía no existe suficiente información disponible que permita valorar de manera concluyente cómo se están aplicando estas facultades frente a vulneraciones de datos personales relacionadas con delitos informáticos. Por esta razón, esta dimensión no puede considerarse plenamente consolidada y requiere un seguimiento posterior que permita evaluar sus resultados concretos.

Respecto de la reparación del daño, el ordenamiento jurídico ecuatoriano reconoce mecanismos de reparación integral tanto en el ámbito constitucional como en el penal. Sin embargo, el análisis realizado no permitió identificar un mecanismo específico y suficientemente expedito que atienda de manera particular los daños ocasionados por el tratamiento ilícito de datos personales mediante medios informáticos. Esto permite advertir una posible distancia entre

el reconocimiento general del derecho a la reparación y la existencia de mecanismos concretos que respondan a las características particulares de este tipo de afectaciones.

En cuanto a la capacidad institucional técnica y presupuestaria, el análisis realizado permitió identificar la necesidad de considerar posibles limitaciones relacionadas con la especialización técnica y los recursos disponibles para las instituciones encargadas de prevenir, investigar y sancionar estas conductas. Sin embargo, al no contar con información suficiente que permita comprobar y medir objetivamente estas limitaciones, no sería adecuado presentarlas como una deficiencia plenamente demostrada. En consecuencia, esta dimensión se mantiene como un aspecto que requiere mayor información y evidencia para determinar su verdadera incidencia en la eficacia del sistema.

Finalmente, respecto de la articulación entre autoridades, el análisis permite identificar esta dimensión como una de las principales debilidades del sistema. La intervención de la Superintendencia de Protección de Datos Personales, la Fiscalía General del Estado y la Policía Nacional responde a competencias diferentes, pero relacionadas cuando un mismo hecho puede involucrar una vulneración de datos personales y la posible comisión de un delito informático. La ausencia de un mecanismo formal que establezca procedimientos claros de coordinación, comunicación y remisión de casos puede generar respuestas fragmentadas o tardías. Esta situación resulta especialmente relevante porque una adecuada protección de los datos personales no depende únicamente de la existencia de normas, sino también de la capacidad de las instituciones para actuar de manera coordinada. Precisamente por esta razón, la presente investigación plantea posteriormente una propuesta jurídica orientada a fortalecer este aspecto.

En conjunto, el análisis realizado permite concluir que el sistema jurídico ecuatoriano de protección de datos personales frente a los delitos informáticos presenta una eficacia parcial. Si bien existe un desarrollo normativo y jurisprudencial importante en cuanto al reconocimiento de los derechos de los titulares y a los mecanismos de tutela jurisdiccional, todavía persisten dificultades relacionadas con la prevención, la capacidad para investigar este tipo de conductas, los recursos y capacidades institucionales y, especialmente, la coordinación entre las autoridades que intervienen en estos casos. Estas limitaciones muestran que el reconocimiento del derecho en la normativa no siempre se traduce en una protección efectiva en la práctica. Por esta razón, los resultados obtenidos sirven de base para la propuesta jurídica planteada a continuación, orientada a fortalecer aquellos aspectos en los que se han identificado mayores debilidades.

2.6 Desarrollo Jurisprudencial

La Corte Constitucional del Ecuador ha ido perfilando, a través de distintos casos, el alcance real de la garantía de hábeas data y su relación con el derecho a la protección de datos personales. El análisis de dos de sus sentencias más relevantes en la materia permite apreciar tanto los avances como las tensiones que enfrenta esta garantía en su aplicación práctica. Cabe señalar que ambas sentencias constituyen precedentes constitucionales relevantes para comprender el alcance del derecho a la protección de datos personales y de la garantía de hábeas data. Sin embargo, no corresponden directamente a casos relacionados con delitos informáticos. Su importancia para esta investigación radica en que permiten comprender con mayor claridad el contenido, alcance y límites del derecho a la protección de datos personales, cuya vulneración puede presentarse precisamente a través de las conductas delictivas analizadas en el capítulo anterior.

En la Sentencia No. 182-15-SEP-CC (2015), el conflicto se originó cuando un exfuncionario del Gobierno Municipal de Mocache solicitó copias del presupuesto municipal, el distributivo de sueldos y las actas donde se había resuelto su propia separación del cargo. Sin embargo, presentó la acción de hábeas data apenas dos días después de haber hecho la solicitud, sin que mediara una negativa expresa de la administración ni hubiera transcurrido el plazo legal para considerarla denegada. Los jueces de instancia le dieron la razón y ordenaron entregar la información, decisión que el Municipio impugnó ante la Corte Constitucional mediante una acción extraordinaria de protección, alegando la vulneración de su derecho a la seguridad jurídica.

El caso plantea así dos problemas jurídicos superpuestos: por un lado, si la sentencia que confirmó el hábeas data sin verificar la existencia de una negativa real vulneró la seguridad jurídica del Municipio; por otro y este es el problema que la propia Corte decide construir de oficio, al advertir un vacío normativo de alcance general, bajo qué criterio debe interpretarse el silencio de la entidad requerida como presupuesto habilitante de la acción. La Corte terminó aceptando la acción extraordinaria de protección presentada por el Municipio y dejó sin efecto las sentencias de instancia, de modo que, en los hechos concretos, el solicitante de la información perdió el caso por haber activado la garantía de forma prematura.

El valor de esta sentencia para la presente investigación no está, sin embargo, en su resultado particular, sino en la regla de alcance general que la Corte fijó con efectos erga omnes: el silencio de la entidad requerida, transcurrido un plazo razonable, debe entenderse como negativa tácita que habilita el hábeas data, de modo que situaciones como la del caso analizado sí quedarían protegidas en el futuro, siempre que el solicitante respete ese plazo. La Corte

aprovechó además el caso para precisar la naturaleza, el contenido y el alcance de esta garantía, estableciendo que su ámbito de protección se circunscribe a la información íntima de la persona asuntos familiares, creencias religiosas, filiación política, orientación sexual, entre otros, cuya divulgación inadecuada pudiera ocasionarle un perjuicio, y no a cualquier documento por el solo hecho de reposar en una entidad pública. Esta precisión resulta especialmente útil para la delimitación conceptual de esta investigación, en la medida en que distingue con claridad la información sujeta a protección de datos personales frente a la información pública o meramente administrativa.

El aporte de este precedente a la pregunta central de la investigación puede entenderse desde dos aspectos. En primer lugar, establece un criterio temporal al considerar el silencio administrativo como una negativa tácita, lo que permite determinar en qué momento el titular puede entender que su derecho ha sido vulnerado y, en consecuencia, recurrir a los mecanismos de tutela correspondientes. En segundo lugar, ayuda a precisar qué tipo de información se encuentra protegida por este derecho. Esta delimitación resulta importante para el desarrollo de la investigación, ya que permite determinar si las conductas informáticas analizadas afectan efectivamente datos personales que cuentan con protección jurídica.

Años más tarde, la Corte Constitucional del Ecuador (2021) mediante la Sentencia No. 2064-14-EP/21, relacionada con la conservación y difusión no consentida de fotografías íntimas, permitió a la Corte profundizar en esta misma línea, pero desde una perspectiva distinta: la del control que conserva el titular sobre su información incluso después de haber autorizado un tratamiento inicial. En ese caso, la Corte determinó la vulneración de los derechos a la protección de datos personales y a la autodeterminación informativa, además de los derechos a la imagen, la

honra, el buen nombre y la intimidad, y afirmó que el titular puede revocar una autorización previamente concedida y exigir la actualización, rectificación o eliminación de su información.

Mientras que la sentencia de 2015 se ocupa de cuándo nace el derecho a activar el hábeas data, la de 2021 aclara qué facultades conserva el titular una vez que la información ya ha sido objeto de tratamiento, configurando así dos dimensiones complementarias de una misma garantía. Este precedente resulta relevante para la pregunta central de la investigación porque permite entender que el derecho a la protección de datos personales no termina con el consentimiento que una persona otorga inicialmente. Por el contrario, el titular mantiene la posibilidad de ejercer un control sobre sus datos y sobre la forma en que estos son utilizados.

Esta consideración es importante para analizar si el ordenamiento jurídico ecuatoriano cuenta con mecanismos adecuados para proteger ese control cuando los datos personales son utilizados o tratados de manera ilícita mediante conductas que pueden constituir delitos informáticos, y no únicamente cuando la afectación se plantea a través de la vía constitucional.

Ambas sentencias muestran que la protección de datos personales en el Ecuador ha alcanzado, en el plano jurisdiccional, un desarrollo doctrinal considerable: la Corte ha delimitado con precisión qué información protege esta garantía, cuándo procede activarla y qué facultades conserva su titular. Sin embargo, el propio caso de 2015 ilustra también el otro lado de esa moneda: una garantía bien diseñada en el papel puede fallar en su aplicación práctica por ambigüedades procesales no resueltas por el legislador en ese caso, la falta de un plazo claro para entender configurada la negativa, obligando a la propia Corte a suplir ese vacío por vía interpretativa. Este patrón, verificado aquí en el terreno de la tutela administrativa y constitucional, es el mismo que la presente investigación busca examinar en el terreno penal: si

el reconocimiento normativo del derecho a la protección de datos personales frente a los delitos informáticos se traduce, en la práctica, en mecanismos claros y oportunos de tutela, o si persisten vacíos similares que exigen ser identificados y corregidos.

2.7 Propuesta jurídica orientada a fortalecer los mecanismos de protección constitucional de los datos personales frente a los delitos informáticos en el Ecuador

El análisis realizado en los apartados 2.5.1, 2.5.2 y 2.5.3 permitió determinar que una de las principales dificultades del sistema jurídico ecuatoriano no se encuentra en la falta de reconocimiento del derecho a la protección de los datos personales, ya que este se encuentra respaldado tanto constitucional como legalmente. La dificultad se relaciona, principalmente, con la forma en que este derecho es protegido y aplicado en la práctica, especialmente en lo referente a la tutela administrativa y jurisdiccional, la capacidad de investigación y la coordinación entre las instituciones que intervienen frente a este tipo de hechos. Estos aspectos fueron considerados en el apartado 2.5 como elementos necesarios para valorar la eficacia jurídica del sistema. A partir de esta realidad, se plantean dos propuestas jurídicas que, aunque pueden aplicarse de manera independiente, se complementan entre sí y buscan fortalecer la protección efectiva de los datos personales frente a los delitos informáticos.

2.7.1 Protocolo de coordinación interinstitucional entre la Superintendencia de Protección de Datos Personales, la Fiscalía General del Estado y la Policía Nacional

El análisis realizado en los apartados 2.5.2 y 2.5.3 permitió observar que la protección de los datos personales frente a los delitos informáticos requiere la participación coordinada de diferentes instituciones. Entre ellas se encuentran la Superintendencia de Protección de Datos Personales (SPDP), encargada del control administrativo; la Fiscalía General del Estado,

responsable de dirigir la investigación penal; y la Policía Nacional, que interviene principalmente en el ámbito técnico e investigativo. Sin embargo, actualmente no se evidencia un mecanismo suficientemente claro que determine cómo debe actuar cada institución cuando un mismo hecho puede generar consecuencias tanto administrativas como penales. Esta situación puede ocasionar que una conducta sea atendida de manera aislada por cada autoridad o que la intervención de una de ellas se produzca cuando ya ha transcurrido un tiempo importante. La falta de una adecuada articulación entre la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal puede afectar, por tanto, la respuesta oportuna frente a conductas que vulneren el derecho a la protección de datos personales.

Frente a esta situación, se propone establecer un protocolo interinstitucional que permita coordinar la actuación y remisión de casos entre la SPDP, la Fiscalía General del Estado y la Policía Nacional cuando un mismo hecho pueda constituir, al mismo tiempo, una infracción administrativa prevista en la LOPDP y un delito informático contemplado en el COIP. Este protocolo debería establecer, de manera clara, los criterios que permitan a la SPDP remitir un caso a la Fiscalía cuando durante una investigación administrativa se identifiquen elementos que puedan evidenciar responsabilidad penal. De igual manera, debería contemplar mecanismos mediante los cuales la Fiscalía pueda comunicar a la SPDP la existencia de investigaciones relacionadas con el tratamiento ilícito de datos personales, con el propósito de que se adopten, cuando corresponda, las medidas administrativas pertinentes. Además, sería necesario establecer canales permanentes de cooperación con la Policía Nacional para facilitar la obtención, conservación y manejo adecuado de la evidencia digital.

La implementación de esta propuesta correspondería principalmente a la Superintendencia de Protección de Datos Personales y a la Fiscalía General del Estado, mediante la celebración de un convenio interinstitucional. La Policía Nacional participaría en aquellos aspectos relacionados con el apoyo técnico y las actividades de investigación que requieran conocimientos especializados en materia de evidencia digital.

La propuesta encuentra sustento en el reconocimiento constitucional del derecho a la protección de los datos personales, establecido en el artículo 66, numeral 19, de la Constitución de la República del Ecuador, así como en la obligación del Estado de garantizar mecanismos adecuados para su protección efectiva. Este planteamiento se relaciona con lo desarrollado por Ferrajoli (2006) y Alexy (2007) en el apartado 2.5, particularmente respecto de la necesidad de que los derechos reconocidos jurídicamente cuenten con mecanismos que permitan hacerlos efectivos. Asimismo, la LOPDP y el COIP contienen disposiciones que permiten la actuación y cooperación de las instituciones involucradas; sin embargo, se considera necesario contar con un instrumento que permita articular estas competencias de manera práctica y ordenada.

El protocolo podría aplicarse mediante un procedimiento previamente establecido para la remisión y seguimiento de los casos, determinando plazos de actuación y designando responsables o puntos de contacto dentro de cada institución. De esta manera, cuando una autoridad identifique hechos que puedan involucrar la vulneración de datos personales y, al mismo tiempo, la posible comisión de un delito informático, la información podría ser trasladada oportunamente a la institución competente. Este modelo permitiría una respuesta más coordinada y evitaría que el titular afectado tenga que enfrentar procedimientos separados sin una adecuada comunicación entre las autoridades. Su lógica de actuación coordinada guarda relación con las

fortalezas identificadas en el modelo español, en el cual la autoridad de protección de datos cuenta con mecanismos que permiten intervenir de manera activa frente a posibles vulneraciones.

2.7.2 Facultad de investigación y auditoría de oficio de la Superintendencia de Protección de Datos Personales

El análisis realizado permitió observar una diferencia importante entre el modelo ecuatoriano y el español. En España, la Agencia Española de Protección de Datos cuenta con una capacidad de actuación preventiva que le permite realizar investigaciones y auditorías de oficio en determinados sectores. En cambio, en Ecuador, la actuación de la SPDP es, en la práctica, principalmente reactiva, ya que interviene generalmente a partir de las vulneraciones denunciadas por los titulares de los datos. Esta situación limita la posibilidad de identificar y atender determinados riesgos antes de que lleguen a afectar los derechos de las personas o de que sus consecuencias se incrementen. Por ello, fortalecer la capacidad preventiva de la autoridad ecuatoriana constituye un aspecto relevante para mejorar la protección efectiva de los datos personales.

Como respuesta a esta situación, se propone fortalecer las facultades de la SPDP mediante el reconocimiento expreso de la posibilidad de iniciar investigaciones y auditorías de oficio, sin que sea indispensable la existencia de una denuncia previa. Esta facultad podría aplicarse especialmente a responsables del tratamiento que desarrollen actividades consideradas de mayor riesgo para la protección de datos personales, como los sectores financieros, sanitario, de telecomunicaciones y determinadas plataformas digitales que manejen grandes cantidades de información personal. Para ello, podrían establecerse auditorías sectoriales periódicas que

permitan identificar deficiencias, prevenir posibles vulneraciones y exigir la adopción de medidas correctivas cuando sean necesarias.

La institución encargada de desarrollar esta propuesta sería la Superintendencia de Protección de Datos Personales, en su calidad de autoridad de control establecida por la LOPDP.

Esta propuesta parte igualmente del reconocimiento constitucional del derecho a la protección de los datos personales y de la obligación estatal de garantizar mecanismos adecuados para su protección. Su implementación podría realizarse mediante una reforma puntual a la LOPDP o a su Reglamento General, con el propósito de establecer de manera expresa el alcance, los límites y el procedimiento para el ejercicio de investigaciones y auditorías de oficio. Si bien el marco jurídico vigente no impide necesariamente una actuación preventiva de la autoridad, resulta conveniente que esta facultad se encuentre desarrollada con mayor claridad para garantizar su aplicación efectiva y evitar interpretaciones que limiten su ejercicio.

En la práctica, la SPDP podría elaborar anualmente un plan de auditorías sectoriales tomando como referencia criterios objetivos de riesgo, entre ellos el volumen de datos tratados, el nivel de sensibilidad de la información, la cantidad de titulares involucrados y los antecedentes de incidentes de seguridad. A partir de estos criterios, la autoridad podría determinar qué responsables o sectores requieren una supervisión prioritaria. Las auditorías permitirían identificar posibles incumplimientos y establecer medidas correctivas antes de que una vulneración genere consecuencias mayores. Esta propuesta toma como referencia la actuación preventiva identificada en el modelo español, pero no pretende trasladar de manera directa el régimen europeo al contexto ecuatoriano, sino adaptar su lógica de supervisión activa a las necesidades y capacidades institucionales de la SPDP.

2.7.3 Elementos complementarios

Las dos propuestas planteadas podrían fortalecerse mediante la incorporación progresiva de otros mecanismos identificados a partir del análisis del derecho comparado. Entre ellos, podría considerarse la creación de un registro público de tratamiento de datos personales, tomando como referencia el modelo colombiano del Registro Nacional de Bases de Datos. Este registro permitiría contar con mayor información sobre los responsables que realizan tratamientos de datos personales y facilitaría la identificación de aquellos sectores o entidades que, debido al volumen o a la sensibilidad de la información que manejan, podrían presentar un mayor nivel de riesgo. A su vez, esta información contribuiría a fortalecer el protocolo de coordinación propuesto, al proporcionar elementos que permitan orientar de mejor manera las acciones de prevención, supervisión y respuesta frente a posibles vulneraciones de datos personales.

En segundo lugar, sería conveniente establecer una cláusula de revisión periódica del régimen sancionador previsto en la LOPDP y el COIP. La evolución constante de la tecnología y de las formas en que se utilizan los datos personales hace necesario que las normas puedan revisarse y actualizarse cuando las nuevas modalidades de afectación así lo requieran. Esta medida permitiría evitar situaciones como la identificada en el caso argentino, donde una legislación que representó un avance importante en su momento enfrentó dificultades para responder adecuadamente a nuevas formas de tratamiento y afectación de los datos personales.

En conjunto, estas medidas buscan que la protección de los datos personales en Ecuador no se limite al reconocimiento formal de este derecho, sino que cuente con mecanismos institucionales capaces de prevenir, detectar, investigar y responder de manera oportuna frente a

las vulneraciones que puedan producirse en el contexto de los delitos informáticos. De esta manera, la propuesta jurídica pretende contribuir a reducir las limitaciones identificadas en la investigación y fortalecer la eficacia práctica de la protección constitucional de los datos personales.

CAPÍTULO III

Metodología

3.1 Enfoque de investigación

La presente investigación se desarrolló bajo un enfoque cualitativo, debido a que se centra en el análisis e interpretación del marco constitucional, legal, doctrinario y jurisprudencial relacionado con la protección de los datos personales frente a los delitos informáticos en el Ecuador. Para ello, se examinaron la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPD), el Código Orgánico Integral Penal (COIP), la jurisprudencia constitucional y la doctrina especializada, con el propósito de determinar en qué medida la articulación de estos instrumentos permite garantizar una tutela efectiva del derecho a la protección de los datos personales frente a los riesgos derivados de los delitos informáticos. La selección del corpus documental respondió a criterios de pertinencia y relación directa con el objeto de estudio, considerando las normas, decisiones jurisprudenciales y aportes doctrinarios necesarios para sustentar el análisis desarrollado.

3.2 Tipo y alcance de la investigación

La investigación tuvo un alcance descriptivo, analítico y propositivo.

Fue descriptiva, porque examinó el marco jurídico ecuatoriano aplicable a la protección de los datos personales, identificando los principios, derechos, obligaciones y mecanismos de

tutela previstos en la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal.

Fue analítica, al estudiar la articulación entre las normas constitucionales, administrativas y penales para determinar si el régimen jurídico vigente garantiza una protección efectiva de los datos personales frente a los delitos informáticos e identificar posibles vacíos o limitaciones.

Tuvo un carácter propositivo, ya que, con base en el análisis normativo, doctrinario, jurisprudencial y comparado, se formularon propuestas orientadas a fortalecer la protección constitucional de los datos personales y la eficacia del sistema jurídico ecuatoriano frente a los delitos informáticos.

3.3 Métodos de investigación

Para el desarrollo de la presente investigación se emplearon métodos propios de la investigación jurídica que permitieron analizar el marco constitucional, legal, doctrinario y jurisprudencial relacionado con la protección de los datos personales frente a los delitos informáticos.

3.3.1 Método jurídico-dogmático

Constituyó el método principal de la investigación, al permitir el análisis e interpretación de la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal, a fin de determinar el alcance del derecho a la protección de los datos personales e identificar posibles vacíos o limitaciones en su regulación frente a los delitos informáticos.

3.3.2 Método analítico

Permitió examinar de manera sistemática las normas, la doctrina y la jurisprudencia aplicables, con el propósito de evaluar la articulación entre la Constitución, la Ley Orgánica de Protección de Datos Personales y el Código Orgánico Integral Penal, así como las fortalezas y limitaciones del sistema jurídico ecuatoriano.

3.3.3 Método hermenéutico jurídico

Se empleó para interpretar el contenido y alcance de las normas constitucionales, legales y jurisprudenciales relacionadas con la protección de los datos personales, considerando especialmente los criterios desarrollados por la Corte Constitucional del Ecuador y la Sentencia No. 2064-14-EP/21.

3.3.4 Método comparado

Permitió contrastar la regulación ecuatoriana con la de España, Argentina, Colombia y Chile, a fin de identificar buenas prácticas que contribuyan al fortalecimiento de la protección de los datos personales frente a los delitos informáticos.

3.3.5 Corpus documental y criterios de selección de fuentes

La aplicación de los métodos descritos requirió precisar el universo de fuentes sobre el cual se aplicaron, así como los criterios utilizados para su selección y su relación con los objetivos específicos de la investigación.

El corpus normativo comprende la Constitución de la República del Ecuador (artículos 66, numeral 19, y 92), la Ley Orgánica de Protección de Datos Personales (particularmente los

artículos 10 y 13 a 21), su Reglamento General y las disposiciones del Código Orgánico Integral Penal directamente relacionadas con la protección de datos personales (artículos 178, 190, 229 y 230 y, de forma complementaria, el artículo 234). El criterio de selección de estas normas es su incidencia directa sobre el bien jurídico de protección de datos personales: se priorizan las disposiciones cuyo objeto de tutela recae de manera inmediata sobre la información personal o la intimidad, y se excluyen aquellas en las que el dato personal opera solo como medio comisivo de otra infracción. Esta normativa responde al primer objetivo específico, orientado a examinar el marco constitucional y legal vigente.

El corpus jurisprudencial comprende las sentencias de la Corte Constitucional del Ecuador No. 182-15-SEP-CC y No. 2064-14-EP/21, seleccionadas por constituir los precedentes más relevantes sobre el alcance del hábeas data y la autodeterminación informativa en el ordenamiento ecuatoriano, y por tratarse de jurisprudencia vinculante emitida por el máximo órgano de interpretación constitucional. Este componente responde al tercer objetivo específico, relativo al análisis de la jurisprudencia relevante.

El corpus doctrinario incluye los trabajos de Ferrajoli (2006) y Alexy (2007), desde la teoría general de los derechos fundamentales; Pérez Luño (2012), Puccinelli (2003) y Westin (1967), en materia de protección de datos, privacidad e intimidad; y Acurio Del Pino (2015), Miró Llinares (2012), Naranjo Godoy (2017), Herrán Ortiz (2003) y Ávila Santamaría (2008), en lo relativo a delitos informáticos y constitucionalismo ecuatoriano. El criterio de selección es la pertinencia temática directa con el problema jurídico planteado y, en el caso de los autores nacionales, su relación específica con el desarrollo dogmático de la protección de datos personales en Ecuador.

Como fuentes oficiales se utilizaron los datos estadísticos de la Fiscalía General del Estado sobre delitos informáticos y la normativa secundaria expedida por la Superintendencia de Protección de Datos Personales, seleccionadas por su oficialidad y por su vigencia al momento del cierre de la investigación, conforme al principio de actualidad normativa que rige este trabajo. Finalmente, el derecho comparado contrastó la regulación ecuatoriana con la de España (RGPD y Ley Orgánica 3/2018), Colombia (Ley 1581 de 2012), Argentina (Ley 25.326) y Chile (Ley 21.719, distinguiendo su régimen vigente de aquel cuya entrada en vigor es posterior), seleccionados por representar distintos niveles de desarrollo institucional en la materia. Este componente responde al cuarto objetivo específico, relativo a la formulación de propuestas jurídicas.

3.4 Técnicas e Instrumentos de investigación

La presente investigación empleó como técnica la revisión documental, por ser la más adecuada para el análisis del corpus normativo, jurisprudencial, doctrinario y comparado definido en el apartado anterior. Mediante esta técnica se recopiló, organizó y analizó la información proveniente de dichas fuentes.

Para la organización y sistematización de la información se aplicaron criterios de análisis documental que permitieron registrar el contenido jurídico relevante de las fuentes consultadas y su relación con el problema y los objetivos de la investigación, así como criterios de análisis comparativo, destinados a contrastar la regulación ecuatoriana con la de España, Colombia, Argentina y Chile, identificando semejanzas, diferencias y buenas prácticas que contribuyan al análisis de la eficacia del sistema jurídico ecuatoriano de protección de datos personales frente a los delitos informáticos

3.5 Procedimiento metodológico

La investigación se desarrolló a partir de la revisión y análisis de las fuentes documentales seleccionadas. La información obtenida fue organizada de manera temática y comparativa, considerando fuentes normativas, jurisprudenciales, doctrinarias y de derecho comparado. Posteriormente, se aplicaron los métodos jurídico-dogmático, analítico, hermenéutico y comparado, lo que permitió examinar cómo funciona la protección constitucional de los datos personales frente a los delitos informáticos, identificar las principales fortalezas y limitaciones del marco jurídico ecuatoriano y, a partir de estos resultados, establecer las conclusiones y propuestas de la investigación.

CAPÍTULO IV

Conclusiones

La presente investigación permitió determinar que la protección constitucional de los datos personales frente a los delitos informáticos en Ecuador presenta una eficacia parcial. Si bien el ordenamiento jurídico reconoce el derecho a la protección de los datos personales y establece mecanismos constitucionales, administrativos y penales para su tutela, el análisis realizado evidencia que persisten limitaciones en su aplicación práctica.

El estudio de las dimensiones de eficacia permitió identificar avances en materia de prevención, protección, tutela, investigación, sanción y reparación, pero también la necesidad de fortalecer las capacidades institucionales y la coordinación entre las autoridades competentes. En

particular, la articulación entre la Superintendencia de Protección de Datos Personales, la Fiscalía General del Estado y la Policía Nacional resulta fundamental cuando una vulneración de datos personales se encuentra vinculada con un delito informático.

Así mismo, se determinó que la evolución de las tecnologías y de las modalidades de afectación de los datos personales exige una respuesta institucional especializada y mecanismos de prevención e investigación que permitan actuar de manera oportuna. En este sentido, la investigación evidencia la necesidad de fortalecer las facultades de control e investigación de la autoridad de protección de datos y establecer mecanismos formales de coordinación interinstitucional.

En consecuencia, se concluye que Ecuador cuenta con una base constitucional y legal relevante para la protección de los datos personales, pero requiere fortalecer su eficacia práctica, especialmente en materia de prevención, investigación y coordinación institucional, con el fin de garantizar una respuesta adecuada frente a las nuevas formas de delincuencia informática.

Bibliografía

- Acurio Del Pino, S. (2015). *Derecho penal informático*. Corporación de Estudios y Publicaciones.
- Alexy, R. (2007). *Teoría de los derechos fundamentales*. (C. B. Pulido, Trad.) Centro de Estudios Políticos y Constitucionales.
- Argentina. (2000). *Ley 25.326 de Protección de los Datos Personales*.
- Argentina. (2001). *Decreto 1558/2001, reglamentario de la Ley 25.326 de Protección de los Datos Personales*. Boletín Oficial de la República Argentina.
<https://www.argentina.gob.ar/normativa/nacional/decreto-1558-2001-70368>
- Asamblea Nacional del Ecuador. (2008). *CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR*.
- Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial.
- Ávila Santamaría, R. (2008). *La Constitución del 2008 en el contexto andino: Análisis de la doctrina y el derecho comparado*. (R. Ávila Santamaría, Ed.)
- Chile. (1999). *Ley 19.628, sobre protección de la vida privada*. Biblioteca del Congreso Nacional. <https://www.bcn.cl/leychile/navegar?idNorma=141599>
- Chile. (2024). *Ley 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*. Biblioteca del Congreso Nacional.
<https://www.bcn.cl/leychile/navegar?idNorma=1209272>
- Colombia. (2008). *Ley 1266 de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales*. Diario Oficial.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488>

Colombia. (2012). *Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

Colombia. (2013). *Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012*. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646>

Corte Constitucional del Ecuador sentencia No. 182-15-SEP-CC, (Corte Constitucional del Ecuador 03 de junio de 2015).

https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoiYm8iLCJ1dWlkIjoiODhmMGY4ZmQtN2YzNS00Y2FhLTkxOWEtNjhjZjE2MDRmZjA2LnBkZiJ9

Corte Constitucional del Ecuador. (2021). *Sentencia No. 2064-14-EP*. Corte Constitucional del Ecuador.

https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoiZDhjYmWl0ZSIInV1aWQiOiI1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRLMC1jNjdmNz
[M1NTMzYjAucGRmIn0=](https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/eyJjYXJwZXRhIjoiZDhjYmWl0ZSIInV1aWQiOiI1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRLMC1jNjdmNz)

Enríquez Álvarez, L. (2017). Paradigmas de la protección de datos personales en Ecuador.

Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales. *FORO. Revista de Derecho*(27).

<https://revistas.uasb.edu.ec/index.php/foro/article/view/500/487>

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

<https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673>

- Ferrajoli, L. (2006). *Derechos y garantías: La ley del más débil*. Trotta.
- Fiscalía General del Estado. (2025). *Analítica de la Fiscalía General del Estado*. Estadísticas de delitos informáticos, acceso no autorizado a sistemas informáticos: <https://www.fiscalia.gob.ec/analitica-noticias-del-delito/>
- Fiscalía General del Estado. (2026). *Instrumento Técnico de Política Criminal: Ciberdelincuencia*. Fiscalía General del Estado. <https://www.fiscalia.gob.ec/wp-content/uploads/2026/01/Politica-Criminal-de-Ciberdelincuencia.pdf?>
- Herrán Ortiz, A. I. (2003). *El derecho a la protección de datos personales en la sociedad de la información*. Universidad de Deusto.
- Miró Llinars, F. (2012). *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*. Marcial Pons Ediciones Jurídicas y Sociales.
- Naranjo Godoy, L. (2017). El dato personal como presupuesto del derecho a la protección de datos personales y del habeas data en Ecuador. *Foro: Revista de Derecho*, (27), 63–82. <https://revistas.uasb.edu.ec/index.php/foro/article/view/501/488>
- Naranjo Godoy, L. (2020). Situación de la protección de datos personales en Ecuador. *Revista Cálamó, Revista de Estudios Jurídicos*, (13), 6–33. <https://doi.org/10.61243/calamo.13.156>
- Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos)*. Diario Oficial de la Unión Europea. <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=es>

- Pérez Luño, A. E. (2012). *Los derechos humanos en la sociedad tecnológica*. Tecnos.
- Puccinelli, O. R. (2003). *Protección de datos de carácter personal: Comentario exegético de la Ley 25.326 y su reglamentación*. Astrea.
- Superintendencia de Protección de Datos Personales. (2026). *Resolución N.º SPDP-SPD-2026-0009-R: Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial*. Superintendencia de Protección de Datos Personales.
- Tribunal Constitucional Federal Alemán. (15 de diciembre de 1983). *Sentencia sobre la Ley del Censo (Volkszählungsurteil)*.
- Westin, A. F. (1967). *Privacy and Freedom*. New York: Atheneum.

DECLARACIÓN Y AUTORIZACIÓN

Nosotros, VEGA NARVAEZ BELÉN ELIZABETH con C.I 0706640430 y PACHECO MENDOZA AQUILES MELQUIADES, con C.I 0911355188 respectivamente, autores del trabajo de titulación: “LA EFICACIA DE LA PROTECCIÓN CONSTITUCIONAL DE LOS DATOS PERSONALES FRENTE A LOS DELITOS INFORMÁTICOS EN ECUADOR”, previo a la obtención del título de Abogado en la Universidad Católica de Santiago de Guayaquil:

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

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

Guayaquil, 23 de agosto de 2026.



f. _____
BELÉN ELIZABETH VEGA NARVÁEZ
C.I: 0706640430



f. _____
AQUILES MELQUIADES PACHECO MENDOZA
C.I: 0911355188

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	La eficacia de la protección constitucional de los datos personales frente a los delitos informáticos en Ecuador		
AUTOR (ES):	Belén Elizabeth Vega Narváez y Aquiles Melquiades Pacheco Mendoza		
REVISOR(ES)/TUTOR(ES)	Mgs. María Paula Ramírez Vera		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia y Ciencias Sociales y Políticas		
CARRERA:	Derecho		
TÍTULO OBTENIDO:	Abogado		
FECHA DE PUBLICACIÓN:	23 de agosto de 2026	No. DE PÁGINAS:	59
ÁREAS TEMÁTICAS:	Derecho constitucional, protección de datos personales, derecho informático, medidas de protección		
PALABRAS CLAVES/ KEYWORDS:	Delitos informáticos, tutela efectiva, eficacia jurídica, prevención, vulneración de derechos, supervisión y control.		

RESUMEN/ABSTRACT (194 palabras):

La presente investigación analizó la eficacia de la protección constitucional de los datos personales frente a los delitos informáticos en el Ecuador, considerando las garantías constitucionales y el marco jurídico vigente. Se empleó un enfoque cualitativo, con alcance descriptivo, analítico y propositivo, mediante los métodos jurídico-dogmático, analítico, hermenéutico jurídico y comparado. Para ello, se examinó la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos Personales, el Código Orgánico Integral Penal, la jurisprudencia constitucional y referentes normativos de España, Colombia, Argentina y Chile. Los resultados evidenciaron que, aunque Ecuador cuenta con una base constitucional y legal importante, persisten dificultades en materia de prevención, investigación y coordinación institucional. En particular, se identificó la necesidad de fortalecer la articulación entre la Superintendencia de Protección de Datos Personales, la Fiscalía General del Estado y la Policía Nacional. Como respuesta, se planteó un protocolo de coordinación interinstitucional y el fortalecimiento de las facultades de la Superintendencia para realizar investigaciones y auditorías de oficio en sectores de mayor riesgo. Se concluye que es necesario reforzar los mecanismos preventivos e institucionales para garantizar una protección más efectiva de los datos personales frente a los delitos informáticos.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR:	Teléfono: +5930963798721 0987423169	E-mail: elizabethvega12001@gmail.com aquilespacheco69@hotmail.com
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	Nombre: Ab. Ángela Paredes Caverro, Mgtr.	
	Teléfono: +593-99 760 4781	
	E-mail: angela.paredes01@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA

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