UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TEMA:

Riesgo en el tratamiento de datos biométricos en servicios digitalizados

AUTORES

Jaramillo Navarrete, Romina Damiany

Mora Cuenca, Naomy Carolina

Trabajo de titulación previo a la obtención del título de

ABOGADO

TUTOR:

Ab. Cuadros Añazco, Xavier Paul

Guayaquil, Ecuador

30 de agosto del 2024

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **Jaramillo Navarrete, Romina Damiany** y **Mora Cuenca, Naomy Carolina**, como requerimiento para la obtención del título de **Abogado.**

TUTOR (A)

XAVIER PAUL CUADROS ANAZCO
Firmado digitalmente por XAVIER PAUL CUADROS ANAZCO
Fecha: 2024.08.26 09:18:09 -05'00'

f. _____
Ab. Cuadros Añazco, Xavier Paul

DIRECTOR DE LA CARRERA

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

Guayaquil, a los 30 días del mes de agosto del año 2024

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, **Jaramillo Navarrete, Romina Damiany**

Mora Cuenca, Naomy Carolina

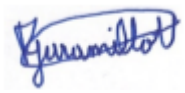
DECLARAMOS QUE:

El Trabajo de Titulación, **Riesgo en el tratamiento de datos biométricos en servicios digitalizados** 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 30 días del mes de agosto del año 2024

AUTORES



f. _____
Jaramillo Navarrete, Romina Damiany

f. _____
Mora Cuenca, Naomy Carolina

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

AUTORIZACIÓN

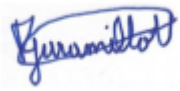
Nosotros, **Jaramillo Navarrete, Romina Damiany**

Mora Cuenca, Naomy Carolina

Autorizamos a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Riesgo en el tratamiento de datos biométricos en servicios digitalizados**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 30 días del mes de agosto del año 2024

AUTORES



f. _____
Jaramillo Navarrete, Romina Damiany

f. _____
Mora Cuenca, Naomy Carolina

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

REPORTE COMPILATIO

CERTIFICADO DE ANÁLISIS
magister

Riesgo en el tratamiento de datos biométricos en servicios digitalizados

3% Textos sospechosos

3% Similitudes
< 1% similitudes entre comillas
< 1% entre las fuentes mencionadas
2% Idiomas no reconocidos (ignorado)
8% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: TRABAJO DE TITULACIÓN-FINAL (1).docx
ID del documento: 9435096e577796b5f789303519b0a02effa39b58
Tamaño del documento original: 2,86 MB
Autor: Romina Jaramillo Navarrete

Depositante: Romina Jaramillo Navarrete
Fecha de depósito: 25/8/2024
Tipo de carga: url_submission
fecha de fin de análisis: 25/8/2024

Número de palabras: 8554
Número de caracteres: 58.625

Ubicación de las similitudes en el documento:

f._____

Jaramillo Navarrete, Romina Damiany

AUTORA

f. _____

Mora Cuenca, Naomy Carolina

AUTORA

XAVIER PAUL CUADROS ANAZCO
Firmado digitalmente por XAVIER PAUL CUADROS ANAZCO
Fecha: 2024.08.26 09:18:09 -05'00'

f. _____

Ab. Cuadros Añazco, Xavier Paul

TUTOR

AGRADECIMIENTOS

A mi familia, que han sido mi pilar fundamental a lo largo de la carrera, por su apoyo y amor incondicional. En especial, mi madre, mi abuela y mi hermana, quienes fueron mi mayor motivación.

A mis compañeros y amigos, Agustín, Gabriela y Rafaella, con quienes compartir un sin número de momentos maravillosos en los pasillos de esta facultad.

A los docentes, Molineros, Mendoza, Benavidez y Cuadros por siempre compartir con paciencia y cariño sus conocimientos.

DEDICATORIA

A los tres pilares de mi vida:

Mi madre, Marjorie Navarrete, la mujer más fuerte y valiente que conozco. Por todo tu sacrificio. Te admiro y te amo demasiado.

Mi abuela, Blanca Saavedra. Por todo su amor, consejos y cuidados.

Mi hermana, Melany Jaramillo. Por siempre acompañarme y guiarme en este largo camino.

Romina Damiany Jaramillo Navarrete.

AGRADECIMIENTOS

A mi padre Ramón Eudoro, mi mejor amigo y guía en este recorrido, quien, con su apoyo incondicional, responsabilidad, sacrificio y esfuerzo logró que pueda cumplir tan anhelada ilusión profesional, gracias por consetir mis aspiraciones y nunca dejar de apostar por mí.

A mi madre Elsa Carmita, mi alma gemela, quien desde su ejemplo me enseño que la nobleza, la humildad y la sencillez te convierten en un ser humano loable en donde sea que te encuentres, gracias a ti, mi mayor admiradora, sé que tuviste miedo de que tome mi rumbo lejos de casa, pero apoyaste el camino que había elegido.

A mi hermana Sharon Noelia, quien desde su incondicionalidad me brinda la seguridad necesaria para creer en mí, por siempre repetirme que podré alcanzar lo que me propusiera, cada logro que tenga en mi vida quiero compartirlo contigo, gracias por hacer de mi felicidad, tu felicidad.

A mi mascota mailo, mi fiel compañerito, desde su llegada a mi vida ha sido un gran apoyo emocional, cuando me sentía sola y lejos de mi familia lo tenía a el para llenarme de mucho amor y alegría.

A Jorge Bueno, quien se convirtió en un elemento clave para mantener en tranquilidad a nuestra familia con sus enseñanzas en fe y sabiduría, gracias por estar presente con un mensaje alentador para mí cuando más lo necesitaba.

A mi abuelita Pepita, quien me esperaba con estusiasmo en casa todas las vacaciones, me recibía con sus abrazos reconfortantes y su alegría única, gracias por hacerme sentir una nieta tan especial y querida.

Finalmente, a todos a quienes formaron parte de esta etapa tan importante en mi vida, el resto de mi familia por enorgullecerse de mí, mis mejores amigas del colegio con quienes he compartido desde que llegamos a una nueva ciudad dejando nuestros hogares para perseguir nuestros sueños, gracias a las personas que conocí en la facultad que se convirtieron en amigos y me dejaron una enseñanza personal para bien, a mi compañera y amiga de tesis por compartir este logro académico junto a mí, gracias a todos los docentes que marcaron y formaron parte de la profesional en la que me convertiré, gracias a mi movimiento político por regalarme una época maravillosa de aprendizaje y alegrías que me llevaré como los mejores recuerdos universitarios, gracias a cada persona que me cruce a lo largo de este recorrido.

DEDICATORIA

Al dueño de la meta de este viaje.

Quien en ningún momento ha soltado mi mano mientras viví este reto tan importante, por ser la inspiración más grande que tengo, por todos aquellos esfuerzos, consejos, y enseñanzas que me dieron la valentía necesaria para no rendirme de ir tras mis anhelos, ni desistir de mis ambiciones, a mi superheroe aquí en la tierra, al mejor amigo, a mi amado padre, esta meta es unicamente por enorgullecerte a ti.

Con amor y gratitud infinita

Naomy Carolina Mora Cuenca

UNIVERSIDAD CATÓLICA

DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

f. _____

LEOPOLDO XAVIER ZAVALA EGAS

DECANO DE CARRERA

f. _____

MARITZA GINETTE REYNOSO GAUTE

COORDINADOR DEL ÁREA

f. _____

EDUARDO XAVIER MONAR VIÑA

OPONENTE

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLÍTICAS
CARRERA DE DERECHO

Facultad: Jurisprudencia
Carrera: Derecho
Periodo: A 2024
Fecha: 25 de agosto 2024

ACTA DE INFORME FINAL

El abajo firmante, docente tutor del Trabajo de Titulación denominado **RIESGO EN EL TRATAMIENTO DE DATOS BIOMÉTRICOS EN SERVICIOS DIGITALIZADOS** elaborado por las estudiantes **ROMINA DAMIANY JARAMILLO NAVARRETE Y NAOMY CAROLINA MORA CUENCA,** certifica que durante el proceso de acompañamiento dichas estudiantes han obtenido la calificación de **(10) DIEZ**, lo cual las califica como **APTAS PARA LA SUSTENTACIÓN**

f. _____
AB. XAVIER PAUL, CUADROS AÑAZCO

ÍNDICE

RESUMEN

El presente trabajo de investigación tiene como objetivo central analizar la normativa ecuatoriana en materia de protección de datos personales, enfocando el objeto de estudio específicamente en el tratamiento de datos personales biométricos en servicios digitalizados, resaltando la falta de regulación conforme a la biometría y los mecanismos de identificación, reconocimiento, autenticación y seguridad biométricos. Destacamos también, la importancia de una normativa que abarque la protección y manejo de los registros y datos biométricos en la actualidad y contexto ecuatoriano, donde vemos cada día como la era tecnológica y digital abunda más en nuestras vidas, creando nuevas problemáticas para el derecho. Y exponemos posibles soluciones a este problema, que puede parecer reciente, pero su evolución crece de forma acelerada y sin embargo en el ámbito internacional, al menos, cuenta con un extenso desarrollo analítico y normativo el cual consideramos puede ser adoptado por la regulación ecuatoriana, ya que esta aún se mantiene limitada.

Palabras Claves: Protección de datos personales, datos biométricos, biometría, seguridad, información, datos sensibles, tecnología, digitalización, consentimiento

ABSTRACT

The central objective of this research work is to analyze the Ecuadorian regulations regarding the protection of personal data, focusing the object of study specifically on the processing of biometric personal data in digitalized services, highlighting the lack of regulation in accordance with biometrics and the mechanisms biometric identification, recognition, authentication and security. We also highlight the importance of regulations that cover the protection and management of biometric records and data in the current Ecuadorian context, where we see every day how the technological and digital era abounds more in our lives, creating new problems for the law. And we present possible solutions to this problem, which may seem recent, but its evolution is growing rapidly and yet in the international arena, at least, it has extensive analytical and regulatory development which we believe can be adopted by Ecuadorian regulation. since this is still limited.

Keywords: Protection of personal data, biometric data, biometrics, security, information, sensitive data, technology, digitization, consent

INTRODUCCIÓN

La legislación ecuatoriana inicialmente establece en la Constitución del año 2008 el derecho a la protección de datos personales en su artículo 66 numeral 19, donde también hace mención del tratamiento de dicha información como la recolección, archivo, procesamiento, distribución o difusión, los cuales requerirán la autorización o consentimiento del titular o el mandato de la ley. A partir de esto, en mayo de 2021, nace la Ley Orgánica de Protección de Datos Personales (LOPDP).

El acelerado avance de la tecnología y su uso en la recopilación de datos ha llegado a tal punto que ahora la mayoría de los dispositivos tecnológicos de uso personal requieren de un reconocimiento automático para su uso, ya sea dactilar o facial. La implementación de estos mecanismos está cada vez más presente en nuestro día a día, tanto en los sectores públicos como privados, pero cuenta la normativa ecuatoriana con una protección suficiente para la creciente afluencia del uso de este tipo de datos personales.

Esta clase de datos personales son de tipo biométrico, los cuales son aquellos que nos identifican como una persona individual y única, diferenciando a cada individuo del resto de la población ya sea mediante su ADN, rasgos faciales, huella dactilar, etc. Es decir, información altamente sensible y en gran cantidad, por ende, tienen un tratamiento especial. El presente trabajo tiene como foco de atención el tratamiento de datos biométricos, considerando que el tratamiento de estos debe cumplir con ciertos parámetros que no se requieren para el manejo de datos personales de carácter más general.

La implementación de datos biométricos puede resultar intrusiva e inclusive en algunos casos vulnerar el derecho a la privacidad e intimidad. A partir de esto, se plantea la interrogante sobre si la normativa ecuatoriana en materia de protección de datos personales cubre todos los aspectos necesarios para su eficaz protección y si contempla los riesgos que el tratamiento de este tipo de datos puede implicar, en el sector tanto público como privado.

CAPÍTULO I

1.1 Importancia de la protección de datos en las sociedades contemporáneas

La protección de datos ha ganado gran relevancia con los avances que han cimentado a las sociedades contemporáneas en virtud de que –a diferencia de otras épocas– nuestra vida cotidiana está estrechamente ligada a la tecnología y esto implica que, además, somos susceptibles a tener potenciales vulneraciones de derechos que antes el imaginario colectivo no podía concebir.

Para el español Moisés Barrio (2021), existen varios autores que consideran que "…los derechos relativos a las tecnologías digitales, el control del cuerpo y la manipulación genética" (p. 27), son parte de una quinta generación de derechos. Es decir, la protección de datos –inmiscuida dentro de las particularidades relativas al régimen de derechos relativos a las tecnologías digitales– ha ganado tanta relevancia a tal punto que las discusiones doctrinales que se creían ya abordadas de manera absoluta, como lo son las generaciones de derechos, se han reabierto al debate.

Dicho esto, es importante tomar en cuenta que las nuevas tecnologías y el accionar de las bases datos, según Pablo Manili (2019), tiene que ver con el derecho a la intimidad, mismo que ha tenido su desarrollo desde mucho antes de que se empezará a discutir sobre los derechos de quinta generación.

Por otro lado, se puede tomar en consideración lo que ara el mexicano Aristeo García González (2007) implica la protección de la información en épocas actuales:

> …con el tratamiento, la recolección, el almacenamiento de informaciones que antes sólo podía formar parte de la vida íntima de cada ser humano –o bien, era conocido por un mínimo sector– ha ido variando paulatinamente su entorno y estructura. Esto es, los datos personales de toda persona se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores tanto públicos como privados (p. 745).

En virtud de estas particularidades que se han suscitado con los avances tecnológicos, el derecho –firme a su finalidad de regular a la sociedad– ha ideado nuevos conceptos y derechos de las personas, con el fin de poder amparar a los individuos y frenar –a través de diversos regímenes– las vulneraciones a derechos que se pueden suscitar.

Es menester indicar que además de restricciones, los ordenamientos jurídicos modernos han contemplado también maneras en las cuales se pueden desenvolver los datos, siendo así que existen normas jurídicas que buscan tutelar, por ejemplo, la privacidad de los datos y, además, poder disponer de estos y alojarlos en bases de datos de una manera que garantice derechos.

Es entonces cuando observamos la necesidad de precautelar la privacidad como base de la protección de datos, siendo esta uno de los derechos conectados directamente con el desarrollo autónomo e integral de cada individuo. Tal como establece el autor José Hernández (2023), "La privacidad es un valor jurídico, fundamento último de la positivización de los derechos fundamentales como la intimidad o la protección de datos personales. Está en su fundamento y orígenes. Este valor jurídico busca el reconocimiento de derechos" (p. 246).

De esta forma, se podría decir que la protección de datos personales es un derecho que se ha desarrollado de manera autónoma, pues, como bien se dijo, fue producto del desarrollo de las tecnologías. Sin embargo, este derecho tiene sus cimientos en el derecho a la privacidad, ya que es considerado como una manifestación de la protección de la vida privada, tal como lo han expresado en su artículo jurídico Vera y Vivero (2019):

> ...la noción de la protección de datos se entiende que es este segmento de la legislación destinado a proteger los derechos fundamentales inherentes a la libertad de los seres humanos, en particular, el derecho a la intimidad individual, respecto del procesamiento de datos, sea manual o automático. (p. 10)

Para autores como el argentino Badeni, el derecho a la privacidad o a la vida privada tiene una gran relevancia en la actualidad. Según Badeni (2006), "El reconocimiento de la libertad de intimidad y el consecuente derecho a la vida privada, configuran un valor que está estrechamente relacionado con la dignidad del ser humano en función de la idea política dominante en las sociedades en vísperas del siglo XXI" (p. 562). En este sentido, se puede aseverar, entonces, que la protección de datos personales está ligada estrechamente con la dignidad del ser humano, en cuanto que la protección de datos personales está sujeto al derecho a la privacidad o el derecho a la vida privada.

Es relevante resaltar que la doctrina ha determinado que los encargados del tratamiento de los datos personales son susceptibles a tener responsabilidades pues, de

hecho, “A medida que las instrucciones otorgadas al encargado del tratamiento sean amplias, mayor será el riesgo para este último de comprometer su responsabilidad” (Cubillos Vélez, 2017, pág. 33). Por ende, la protección de datos personales ostenta tal relevancia que incluso los ordenamientos jurídicos prevén responsabilidades para quienes se encargan del tratamiento en caso de no hacerlo de manera correcta, en tal razón que incluso se puede observar que existen tipificaciones de índole penal que buscan tutelar los datos personales como un bien jurídico protegido.

1.2 Generalidades del derecho a la protección de datos personales

Los datos personales son “cualquier información relativa a una persona física identificada o identificable” según artículo 2 literal a del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (1981). Así, al ser tan amplia la información que otorga el dato personal esta puede ser usada de diferentes maneras, lo que se le conoce como su “tratamiento”, creando una necesidad de protección para el titular de la información. De este modo, el tratamiento de datos personales se traduce como cualquier uso, operación o conjunto de operaciones realizadas sobre datos personales, mediante procedimientos automatizados o no.

Partiendo de esta aclaración, surgen las figuras del titular y el responsable. El titular del derecho es aquella persona natural cuya información es objeto de tratamiento, y el responsable de datos es quien recopila la información entregada y decide cómo usarla o tratarla.

El derecho a la protección de datos personales –mismo que está inmerso dentro de la quinta generación de derechos– está contemplado en la Constitución ecuatoriana en el numeral 19 del artículo 66 de la Constitución e incluye el acceso y decisión sobre información y datos de ese carácter. Esta acepción se la puede complementar con el siguiente criterio de la Corte Constitucional del Ecuador en la sentencia No. 1868-13-EP/20 (2020):

> …el concepto de datos personales incluye datos sensibles relativos a la vida privada y familiar de la persona, pero también información sobre cualquier tipo de actividad desarrollada por ella, como la referida a sus relaciones laborales, económicas o sociales, con independencia de su posición o capacidad (por ejemplo: como consumidor, paciente, trabajador por cuenta ajena, cliente, entre otras) (pág. 6).

Complementariamente a esto, es importante denotar que, para la Corte Constitucional del Ecuador en su sentencia No. 2064-14-EP/21 (2021), cuando se habla de las actuaciones relativas a los datos personales según lo contemplado en el numeral 19 del artículo 66 de la Constitución, existen elementos que son indispensables:

> … todas estas actuaciones (las mencionadas en el numeral 19 del artículo 66), requieren de autorización legal o del titular; sin embargo, aun cuando el titular haya autorizado estas acciones, aquel no pierde la titularidad sobre sus datos personales, motivo por el cual, puede revocar su autorización en cualquier momento (pág. 21).

A raíz de este criterio de la Corte Constitucional, es posible comprender la magnitud que tiene la protección de datos personales como derecho y, por ello, resulta imperioso que las normas jurídicas que se encarguen del tratamiento de estos sean precisas y logren garantizar la plena vigencia de este derecho.

1.3 Elementos de la protección de datos personales

1.3.1 Principios fundamentales para la protección de datos

El Comité Jurídico Interamericano de la Organización de Estados Americanos adoptó la propuesta de declaración de Principios de privacidad y protección de datos personales en las Américas (2021), en donde establece ciertos principios básicos que junto con demás estándares internacionales conforman una pauta que facilita la protección de datos personales, a la vez que guía a los Estados hacia un modelo a seguir con respecto al tratamiento de datos.

Esta misma declaración de principios por parte de la OEA, fue adoptada por la LOPDP, como se menciona en sus considerandos y podemos destacar la presencia de estos principios en el artículo 10 de dicha ley:

Principio de Transparencia y consentimiento

Se deberá especificar la información de datos de contacto del responsable de los datos, la finalidad por la cual se tratarán los datos personales, su fundamento jurídico, destinatarios, la información transmitida y los derechos del titular en relación con los datos recopilados. Cuando se requiera consentimiento para el tratamiento de

datos, este deberá ser solicitado previo a la recopilación de los datos. Además, este consentimiento deberá ser inequívoco, libre e informado.

Principio de pertinencia, necesidad y minimización

Los datos personales serán aquellos considerados adecuados, pertinentes y limitados al mínimo necesario para las finalidades específicas de sus recopilación y tratamiento.

Principio de tratamiento y conservación limitados

El tratamiento y conservación de los datos personales será de manera legítima no incompatible con las finalidades para las cuales fueron recopilados. Su conservación no se extenderá del tiempo necesario para cumplir con sus finalidades y según la legislación de cada Estado.

Principio de confidencialidad

Los datos personales no deberán ser divulgados, no deberán estar a disposición de terceros, ni serán empleados para finalidades diferentes a las cuales fueron motivo de su recopilación, exceptuando los casos en los que el titular conceda su consentimiento o bajo la autoridad de la ley.

Principio de seguridad

La seguridad de los datos personales contra tratamientos no autorizados o ilegítimos deberá proteger la confidencialidad, integridad y disponibilidad de estos, incluyendo los casos accidentales en donde el tratamiento de datos se vea afectado, deberá garantizarse mediante salvaguardias, las cuales deberán ser auditadas y actualizadas de forma permanente.

Principios de acceso, rectificación, cancelación, oposición y portabilidad

Los Estados tendrán que disponer de mecanismos razonables, ágiles, sencillos y eficaces para el acceso, rectificación y cancelación de los datos de aquellos que así lo soliciten. Además, el derecho a oponerse a su tratamiento y, en lo aplicable, el derecho a la portabilidad de esos datos personales.

Principio de responsabilidad

Para garantizar que el tratamiento de los datos se realizará conforme a los principios, la implementación de medidas técnicas y organizacionales que sean apropiadas y efectivas por parte de los responsables del tratamiento y recopilación de datos personales. El responsable deberá cooperar, a petición de las autoridades, en el ejercicio de sus tareas.

1.3.2 Tipos de datos personales

La principal categoría para definir a los datos personales es el carácter sensible de estos. Es decir, existe una distinción entre aquellos datos personales sensibles y los que no lo son. Los datos personales no sensibles son aquellos que no se encuadran dentro de una categoría especializada que requiera de protección y tratamiento diferenciado, debido a su carácter general. Estos pueden ser:

- Patrimoniales: Cuentas de banco, ingresos y egresos económicos, existencia de bienes, número de bienes que posee;
- Académicos: registro de calificaciones, títulos obtenidos, seminarios, lugar donde se estudió, etc.;
- Identificación: nombre, teléfono celular, email, número de cédula, domicilio, etc.

Mientras que en los datos sensibles podemos encontrar:

- Salud: Historial clínico, enfermedades; Físicos: Datos genéticos, ADN, datos biométricos;
- Ideológicos: Religión, ideología, filiación política;
- Culturales: Etnia, nacionalidad, lengua, comunidad;
- Civiles: Condición migratoria, pasado judicial, género, etc.

Este tipo de datos se los encuadra como sensibles debido a que son de extremo cuidado y deben tener un tratamiento especial, ya que afectan directamente al desarrollo de la personalidad. En los ejemplos puntualizados ponemos ver datos sensibles que no solo afectan el desarrollo de la personalidad de los individuos, si no también datos que conforman la vida privada de estos. Es así, que según el tipo de

información y cuanta de esta se tenga, los datos personales pueden llegar a ser considerados como “de naturaleza altamente personal y sensible”.

La presente investigación se centra en el tratamiento de datos biométricos, los cuales según nuestra ley LOPDP en el artículo 4, son únicos y hacen referencia a “las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme su identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros” (Ley Orgánica de Protección de Datos Personales, 2021). Es decir, son considerados como altamente sensibles, por ende, tienen un tratamiento especial. Al tratarse de datos personales que requieren un tratamiento especial, por el tipo y cantidad de información que manejan, la implementación de datos biométricos puede resultar intrusiva e inclusive vulnerar el derecho a la privacidad e intimidad.

La información que contienen estos datos está relacionada con características conductuales o fisiológicas de un individuo que se utiliza para su identificación. Estos datos pueden incluir varios elementos, dependiendo del tipo de tecnología biométrica utilizada. Algunos tipos comunes de los datos biométricos son:

- Identificadores biométricos fisiológicos
- Reconocimiento Facial: Características faciales, como la forma y disposición de los ojos, la nariz y la boca. Patrones únicos, como la textura de la piel y las líneas faciales.
- Huellas Dactilares: Patrones únicos de crestas y valles en las yemas de los dedos. Minucias, que son puntos específicos donde las crestas se bifurcan o convergen.
- Reconocimiento de Iris: Patrones únicos en el iris del ojo. Características como la textura y los detalles del patrón del iris.
- Identificadores biométricos conductuales:
- Reconocimiento de voz: Características vocales, como tono, velocidad, entonación y otros aspectos relacionados con la voz. Patrones únicos en la forma en que se pronuncian palabras o frases.
- Teclas Dynamic: Se usa el patrón de escritura del usuario para identificar intentos de acceso malintencionados o actividades sospechosas en línea.
- Firma digital: Se usa la escritura única de una persona para autenticarla. (ARATEK, 2023)

1.4 El ordenamiento jurídico ecuatoriano y la protección de datos personales

Como bien se ha podido constatar, existe una vasta conceptualización en torno a los datos personales, en tanto que no es un asunto ligero de regular o salvaguardar. Por ello, para poder tutelar un derecho constitucional hace falta que exista una norma infraconstitucional que le otorgue la eficacia que carecería este derecho si se lo quiere aplicar por sí solo, en tanto que son las normas infraconstitucionales las que orientan la conducta de los individuos dentro de la sociedad.

En otras palabras, es importante denotar que, si bien pueden existir preceptos normativos positivizados en la Constitución y desarrollados por la jurisprudencia de la Corte Constitucional o por la doctrina, estos de nada sirven si es que no tienen una aplicación práctica, es decir, no generan los efectos deseados en la sociedad que quieren regular; para el autor ecuatoriano Iván Castro Patiño (2004) existe un tipo de normas jurídicas que se acoplan a esta situación: Existen la normas programáticas que "Son reglas constitucionales no autoaplicativas o no autooperativas. Requieren ser reglamentados por ley para entrar en funcionamiento" (p. 63).

En el caso particular de la protección de datos, no existía una norma especializada que se encargue de viabilizar de manera correcta el funcionamiento de los preceptos jurídicos generales contemplados en el numeral 19 del artículo 66 de la Constitución. Tal era la situación, que en septiembre de 2019 el país sufrió una masiva filtración de datos personales, la cual pasó a la historia debido a que se filtró información personal de toda la población. Sin embargo, no fue sino hasta el 26 de mayo de 2021 el momento en el cual se incorporó al ordenamiento jurídico una norma infraconstitucional encargada de regular y precautelar el derecho de la protección de datos personales; la norma es la Ley Orgánica de Protección de Datos Personales (LOPDP) que se promulgó en el Quinto Suplemento del Registro Oficial No. 459. Es decir, recién en el año 2021 se buscó regular de una manera concreta el derecho de la protección de datos personales.

Los objetivos principales de la LOPDP son garantizar los derechos de acceso y decisión sobre los datos personales, de la mano con su protección mediante la determinación y desarrollo de principios, derechos, obligaciones y mecanismos de tutela. Para ello, también se ha desarrollado un reglamento para esta ley, el cual fue promulgado en el Registro Oficial Tercer Suplemento 435 del 13 de noviembre de

2023. Así, el reglamento funciona como una norma complementaria para ampliar la protección al derecho a la privacidad.

Ahora bien, no por ello se debe de obviar la existencia de garantías jurisdiccionales tales como el habeas data que, para autores como Santiago Velásquez Velásquez, (2010) constituyen la garantía idónea para la tutela de los derechos contemplados en los numerales 19 y 20 del artículo 66 de la Constitución de la República. Sin embargo, es importante reconocer la importancia de la existencia de las normas infraconstitucionales, tales como la LOPDP, en tanto que esta clase de normas especializadas en el tema tienen la vocación de otorgar pautas más concretas para el ejercicio y la protección de este derecho en el Ecuador, en comparación del habeas data, por ejemplo.

Dicho esto, es relevante denotar que el legislador ecuatoriano suele tener errores a la hora de plantear conceptos y pautas con las cuales diversos derechos se desenvuelven en nuestro ordenamiento jurídico a través de normas infraconstitucionales. Es decir, pueden existir contradicciones o vacíos normativos que al final no logren contemplar todos los hechos hipotéticos que ameritan una regulación y esto puede traer conflictos a la hora de ejercer o proteger los derechos.

CAPÍTULO II

El tratamiento de datos biométricos en servicios digitalizados

2.1 Afectaciones al derecho a la privacidad

Actualmente, los datos biométricos se convirtieron en un elemento esencial de todos aquellos sistemas de identificación; debido a su particularidad y autenticidad, son únicos e irrepetibles para cada ser humano, entre estos, como hemos mencionado con anterioridad, las huellas dactilares, el reconocimiento facial y patrones de iris. Es decir, son mayormente usados como mecanismos de registro en sistemas para garantizar un acceso seguro.

La recopilación de datos biométricos de este tipo, como lo son huellas dactilares, escaneo de iris y retina, imágenes fáciles, ente otros, conlleva la transformación de características físicas únicas de una persona en datos digitales, dando como resultado la "datificación" del ser humano, esta información por la general es almacenada en plantillas que servirán para la identificación. Y como las características y rasgos que permiten la identificación de forma única de una persona son parte del cuerpo de ese ser, su recolección y uso podrían interferir con la autonomía personal del ser humano y dignidad. Debido a que una vez creada la plantilla biométrica esta se almacenará en una base de datos, y cualquier persona con acceso a la base de datos o a las plantillas será capaz de no solo identificar sino también de rastrear al usuario o titular en cualquier parte del mundo, creando graves riesgos y vulnerando un sin número de derechos. Produciendo así una pérdida de control la información y características físicas y corporales de una persona. El traspaso de características biométricas a datos digitalizados puede significar la objetivación del cuerpo humano, lo exponen a su uso y a varios riesgos para fines propios de quien posea la información, incluso si estos fines están en contradicción con los intereses del interesado (Wendehorst y Duller, 2021).

El manejo y uso de los datos biométricos debe ser especial en términos de privacidad y seguridad. Uno de los principales riesgos del manejo de estos datos puede ser su uso indebido. Este tipo de datos sensibles están en riesgo y esto se acentúa por la implementación de marcos legales que, si bien buscan proteger la identidad de los

ciudadanos, a menudo presentan vacíos que podrían comprometer la integridad de la información sensible.

En Ecuador, se emitió la Resolución Nro. 003-NG-DINARP-2022 sobre el Funcionamiento del Sistema de Autenticación Única (SAU), en el Registro Oficial No. 123, de agosto de 2022. Ha sido un paso hacia la protección de la privacidad de los ciudadanos. No obstante, esta resolución contiene vacíos legales que limitan su efectividad, ya que es muy general en su contenido y no aborda en una totalidad la información necesaria respecto al uso de datos en el Sistema Nacional de Registros Públicos o, en este caso, sobre los datos para el acceso a este sistema de autenticación.

Por ejemplo, la resolución carece de disposiciones claras sobre la responsabilidad en caso de filtraciones de datos, así como sobre la destrucción segura de la información una vez que ha cumplido su propósito o terminada la relación laboral existente. Además, esta no establece un límite con respecto de la cantidad y tipo de información que se puede llegar a recopilar, ya que el usuario podría estar dando más información de la requerida, o inclusive más de la que está dispuesto a dar y no tener conocimiento de esto, vulnerando así uno de los principios fundamentales como el de minimización y necesidad de la información. Exponiendo otros riesgos, la normativa no contempla adecuadamente las tecnologías emergentes y los nuevos métodos de recopilación de datos biométricos, lo que podría dejar a los ciudadanos desprotegidos frente a futuras amenazas por la inexistencia de garantías.

Otro de los principales riesgos asociados con el trato de los datos biométricos radica en las consecuencias de una afectación al derecho de la privacidad. Por ejemplo, a diferencia de las contraseñas, números o códigos de identificación que pueden ser modificados en caso de accesos no reconocidos o indebidos, los datos biométricos, una vez comprometidos, no pueden ser alterados debido a su autenticidad ya que una persona no puede cambiar sus características físicas y por ende tampoco las biométricas. En contraste con otros datos personales, como el número de la seguridad social, identificación o la dirección, no están indisolublemente ligados a las características físicas del individuo, sino que sólo está vinculados de manera contingente a una persona. Esto los convierte en un objetivo atractivo para actividades ilícitas como el robo de identidad, el fraude financiero y la vigilancia no autorizada.

Si bien, los mecanismos de seguridad biométrica son principalmente usados para la identificación, control de acceso y autenticación en plataformas digitales para accesos y autorización, y por su dificultad para ser descifrados en comparación con cualquier otro mecanismo de seguridad. Pueden resultar como un arma de doble filo debido a que expone a los usuarios a una mayor vulneración de su privacidad si se produce una violación de datos que deje expuestas sus credenciales biométricas (Molinaro, 2022).

A partir de esta idea, es importante mencionar lo que ocurrió con el proyecto Worldcoin de la empresa extranjera privada que mediante dispositivos Orbs escanea el iris de personas, esto ocurrió recientemente en las ciudades de Quito y Guayaquil, en donde los ciudadanos a cambio de permitirse escanear voluntariamente el iris recibían una remuneración económica de 20 criptomonedas, generando una ola de preocupación en los expertos en protección de datos, ya que existe un desconocimiento respecto al riesgo asociado con la entrega de los datos biométricos.

Adicionalmente, se cuestiona mucho la falta de transparencia en la gestión y almacenamiento de datos por parte de esta empresa. Ecuador enfrenta muchos desafíos en cuanto a la falta de regularización y protección de datos. El mal manejo de estos datos puede traer consigo la consecuencia más grave como la pérdida de control sobre la propia identidad, exponiendo a los individuos a una serie de vulnerabilidades que pueden tener consecuencias duraderas. Otro punto por destacar es la poca información que dan las entidades sobre la fiabilidad y precisión de las tecnologías y algoritmos usados para la recolección de datos tan sensibles por parte de empresas como Worldcoin, lo que causa un gran desconocimiento para los usuarios, provocando así una vulneración a los principios de transparencia y consentimiento.

En definitiva, los servicios públicos y privados que están digitalizados al implementar el uso de los datos biométricos ofrecen numerosas ventajas de eficiencia y avances digitalizados. Su manejo inadecuado puede acarrear riesgos significativos para la privacidad y seguridad de los individuos. Por lo tanto, es crucial que se tomen medidas adicionales para cerrar los vacíos legales existentes y asegurar que la protección de los datos biométricos sea completa y adecuada, preservando así los derechos fundamentales de los ciudadanos en el entorno digital.

2.2. Protección de datos biométricos en la LOPDP

La Ley Orgánica de Protección de Datos Personales (LOPDP) abarca una serie de aspectos bastante amplios en el sentido de principios, derechos, seguridad, responsabilidades, sanciones, obligaciones, deberes, entre otros. Sin embargo, como hemos mencionado, se han generado interrogantes en lo que corresponde al tratamiento de datos personales de carácter biométrico, ya que su uso en la actual era digital crece a gran demanda. Si bien la ley define los datos biométricos y los categoriza como sensibles en su artículo 4, no existe gran mención de ellos, lo cual genera una preocupación, ya que este tipo de información no cuenta con una regulación específica y robusta, más allá de lo establecido en la LOPDP y en su reglamento. Es decir, no ha profundizado sobre el uso de la biometría a pesar de que los ha categorizado como datos sensibles en su artículo 25 y por ello tienen un tratamiento especial y diferenciado como establece el artículo 26, que a pesar de que prohíbe el tratamiento de datos personales sensibles en su literal a) exceptúa esta prohibición en caso de obtener el consentimiento explícito del titular.

Por esta razón, es importante destacar los criterios generales que contempla la ley para el tratamiento de datos biométricos, y establecer cómo, a pesar de que estos criterios contienen una serie de principios fundamentales que previenen y conservan la seguridad de datos, al tratarse de datos tan sensibles, cuyo desarrollo se encuentra en constante evolución y cuya seguridad enfrenta nuevos riesgos y vulneraciones cada día, la normativa ecuatoriana no puede solamente considerar como únicos estos criterios y condiciones. Es de suma importancia que los estándares para el tratamiento de datos biométricos en la regulación ecuatoriana sean más estrictos, sobre todo por su creciente empleo como mecanismos de seguridad (Aguirre, 2023)

2.2.1 Consentimiento e interés legítimo

En ese mismo artículo 4, anterior a la definición de dato biométrico, encontramos la definición que le otorga la LOPDP al consentimiento. Se establece que se configura como la “Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos”. Cuando se otorga el consentimiento para el tratamiento de datos biométricos, las finalidades para su uso

pueden ser muy amplias, permitiendo un manejo que probablemente se desconoce o ignora. (Ley Orgánica de Protección de Datos Personales, 2021)

La siguiente mención que nos hace la ley sobre el consentimiento es en el artículo 7 sobre la legitimidad del tratamiento de datos personales, en su numeral 1, donde contempla al consentimiento como una de las condiciones para el tratamiento legítimo y lícito de datos. Posteriormente, el artículo 8 de la ley establece los criterios de validez del consentimiento.

Para continuar, es menester mencionar que el consentimiento se traduce como la manifestación de la voluntad. Esta, a su vez, les da la facultad a las personas de crear relaciones jurídicas mediante su expresión, facultad que debe ser protegida de la propia ignorancia y desconocimiento de las personas y de la influencia y desinformación de terceros que pueden alterar la voluntad. (Stolfi, 2018)

Por ende, es necesario que exista un nivel de conciencia y voluntad, ya que los actos jurídicos no se completan solamente con el acuerdo de las partes para manifestar su voluntad. Esto es esencial para que el acto no sólo tenga efectos jurídicos, sino también para que carezca de vicios que puedan llevar a su nulidad total o parcial. (Llanos, 1944)

A partir de esto, como mencionamos con anterioridad, el consentimiento es la manifestación de la voluntad libre, específica, informada e inequívoca según nuestra ley. Por esta razón, es necesario que las instituciones tanto públicas como privadas que busquen tratar datos biométricos se aseguren de proporcionar a sus usuarios en sus políticas, antes del uso de datos, información como:

- Explicación detallada del tipo de datos y uso específico, y el motivo y finalidad del tratamiento
- El nivel de fiabilidad y precisión del algoritmo utilizado

Estos parámetros no están contemplados expresamente en la LOPDP, permitiendo un tratamiento más amplio, lo que puede ocasionar posibles vulneraciones. Además, la autoridad de protección de datos debería encargarse de que las instituciones cumplan efectivamente con esto en sus políticas, en adición con posibles obligaciones como:

- Auditar los sistemas
- La trazabilidad del proceso
- Demás garantías

Estos cuatro criterios de la manifestación de la voluntad son de fundamental cumplimiento, ya que en caso de que no se cumpla con alguno de ellos el consentimiento carecería de validez; por ende, se caería en un acto ilegítimo e ilícito al tratar datos bajo condiciones que no son contempladas por ley, vulnerando así la protección y privacidad de los datos. Es por esto por lo que los datos biométricos deben tener un grado más elevado de protección.

Por otra parte, con respecto al uso específico, motivo y finalidad del tratamiento, esto debe ser transparente para el titular, de forma que quede clara la necesidad del tratamiento de estos datos para fundamentar el interés legítimo del responsable del tratamiento o de terceros. Tanto el interés legítimo como el consentimiento explícito se encuentran directamente relacionados a la hora de proteger datos. Sin embargo, el tratamiento de datos biométricos contiene varios matices y no deberían ser los únicos aspectos por considerar para permitir el tratamiento de datos biométricos.

2.2.2 Necesidad y proporcionalidad

Por otro lado, el tratamiento de datos personales debe ser necesario y proporcional al fin legítimo que la entidad que trata los datos debe especificar. Esto quiere decir que los encargados de los datos únicamente podrán tratarlos, si su uso va de acuerdo con las finalidades específicas para su recopilación. En razón a esto, se debe seguir el estricto criterio de minimización, el cual establece que los encargados únicamente deberán recopilar la información mínima requerida para las finalidades específicas.

Ahora bien, hablando del manejo de datos en instituciones del sector público y su finalidad, aparece el término “proporcionalidad”, el cual determina:

> sí una medida ha ido más allá de lo que se requiere para alcanzar una finalidad y si los beneficios alegados excederán los costos previstos. En el contexto del Tratamiento de Datos del sector público, la idea de necesidad a veces se mide sobre la base de la proporcionalidad; por ejemplo, al exigir un equilibrio entre 1) el interés

del público en el Tratamiento de los Datos Personales y 2) la protección de los intereses de las personas en materia de privacidad. (Organización de los Estado Americanos (OEA), 2021)

Es así, como estos conceptos ponen límites al tratamiento de datos personales. Sin embargo, como lo discutimos en el apartado anterior, esto puede cambiar si el titular otorga el consentimiento para el tratamiento. Por ende, surge la pregunta sobre si los preceptos descritos anteriormente son suficientes para proteger los datos biométricos, al ser estos cada vez más usados como mecanismos de seguridad digital y tecnológica. Resaltando así, la importancia de la evolución en la legislación para que alcance a proteger este tipo de información.

Por los motivos expuestos, es responsabilidad del Estado establecer salvaguardias para la protección de datos y un constante revisión y supervisión de los métodos y mecanismos de recopilación. La implementación de un marco regulatoria de incluya estas obligaciones, en específico para datos biométricos, es muy necesaria. Y queda demostrado con los recientes acontecimientos con respecto al proyecto Worldcoin, que el país se encuentra muy expuesto a injerencias indebidas al derecho a la privacidad.

2.3. Guías y medidas de protección de datos personales

La biometría se ha convertido en un elemento clave para el desarrollo digitalizado en muchos países, incluyendo el nuestro. Pese a que existen herramientas para la identificación y autenticación personal como hemos mencionado, el presente trabajo reúne que Ecuador aún carece de una legislación sólida en lo que respecta a este tipo de datos. Sin embargo, países como México y España cuentan con manuales específicos para el tratamiento de los datos biométricos; aquí compararemos las medidas de alcance de la protección de datos sensibles en los países anteriormente mencionados, respecto a la situación actual en Ecuador, destacando la urgente necesidad de un marco legal adecuado.

2.3.1 Guías y Medidas de Protección de Datos Biométricos Europa

En mayo del año 2018, se actualizó el Convenio 108 suscrito por el Consejo Europeo, que tiene por nombre Convenio para la protección de las personas con el respecto al tratamiento de datos personales. En este tratado internacional que establece

principios fundamentales para la protección de datos personales, en su artículo 6 se da énfasis especial en la protección de los datos sensibles, el cual establece que dichos datos deben ser tratados bajo condiciones específicas que ofrezcan garantías, protegiendo así los derechos fundamentales de cada individuo y también se asegure un elevado nivel de privacidad en el tratamiento de este tipo de información. Los países de América suscritos al Convenio 108 han sido hasta la actualidad Argentina, Uruguay y México, dando pasos agigantados en lo que respecta a las garantías sobre la protección de datos personales. Así mismo, este convenio y demás cuerpos normativos han sido elaborados según una serie de estudios a cargo del Parlamento Europeo que otorgan una base científica a sus regulaciones, muchos sobre avances tecnológicos y protección de datos, por ejemplo, el estudio sobre el Reconocimiento biométrico y detección de comportamientos sospechosos (Biometric Recognition and Behavioural Detection).

2.3.2 Guías y Medidas de Protección de Datos Biométricos en España

En España, se ha establecido un amplio marco para la protección de datos. El Reglamento General de Protección de Datos clasifica los datos biométricos como datos sensibles y establece requisitos estrictos para su tratamiento. Las entidades autorizadas que manejen datos biométricos deben obligatoriamente justificar la necesidad de la recolección y tratamiento, asegurando que no existen otras alternativas menos invasivas para lograr los fines propuestos para el uso de estos datos.

Además, es importante mencionar que existe un ente como la Agencia Española de Protección de Datos (AEPD), quienes emitieron una guía específica sobre el tratamiento de datos biométricos, enfatizando la importancia de la minimización de datos, es decir, que solo se deben recolectar y procesar solo los datos estrictamente necesarios. También se destacan las obligaciones de transparencia y de proporcionar a los individuos información clara sobre el uso de sus datos biométricos, así como el derecho a retirar su consentimiento en cualquier momento**.**

2.3.3 Guías y Medidas de Protección de Datos Biométricos en México

Este país ha avanzado de forma significativa en la protección de datos personales biométricos a través de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su respectivo reglamento. El Instituto

Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) emitió una respectiva guía donde se establece cómo deben manejarse los datos biométricos, reconociéndose como datos sensibles que requieren un nivel de protección y tratamiento especial.

Las guías del INAI recomiendan que las empresas privadas y entidades públicas adopten medidas de seguridad técnicas y organizativas para proteger los datos biométricos, como la encriptación, el control de acceso y la implementación de políticas de privacidad robustas. Además, se exige que los responsables del tratamiento de estos datos obtengan el consentimiento explícito e informado de los individuos antes de recolectar y procesar sus datos biométricos, lo cual garantiza un mayor control por parte de los titulares sobre sus propios datos.

2.3.4 Normativa ecuatoriana

En un cuadro comparativo en cuanto a los países de México y España, estos se encuentran altamente actualizados en lo que respecta al trato de datos biométricos. A diferencia de Ecuador, que no cuenta con una especificidad del tratamiento de los datos mencionados, en el 2021 se dio paso a gran paso con la expedición de una Ley Orgánica de la Protección, como los hemos mencionado, sin embargo, no se logra abordar de manera explícita los riesgos y particularidades que se encuentran arraigados al manejo de los datos biométricos.

Ecuador aún se encuentra en una etapa rudimentaria, con una legislación que no aborda de forma completa los desafíos y riesgos asociados con el tratamiento de los datos biométricos y su afectación a la privacidad y seguridad de cada individuo. Es importante que nuestro país se homogenice en un avance normado para fortalecer y proporcionar un marco seguro para que tanto empresas, como organizaciones y las distintas entidades manejen de forma apropiada y correcta esta información sensible. La implementación de garantías, reglas y reformas sería esencial para garantizar que Ecuador se alinee con los estándares globales apropiados para asegurar un correcto, ético y seguro uso de la información biométrica de la ciudadanía.

CONCLUSIONES

Es evidente que los datos personales biométricos son inherentemente sensibles y únicos para cada persona, la recolección y tratamiento de estos datos plantea importantes desafíos en términos de privacidad y seguridad. Como hemos mencionado a lo largo de este trabajo, existe un alto riesgo de abuso, desde la suplantación de identidad hasta el acceso no autorizado a información personal, al ser utilizados, lo que puede causar daños irreparables a los afectados. En Ecuador, el peligro se intensifica debido a la falta de mecanismos adecuados de protección de datos personales, a pesar de la sensibilidad de los datos biométricos.

Se puede concluir, que la falta de directrices claras y la implementación insuficiente de medidas de seguridad en la ley y su reglamento plantean preocupaciones sobre la capacidad del marco legal para proteger adecuadamente la privacidad de los individuos. En ausencia de controles organizativos y técnicos estrictos, los datos biométricos pueden estar expuestos a riesgos que pueden comprometer la privacidad del individuo y la seguridad de las instituciones que los manejan este tipo de datos.

Aunque la ley constituye un paso importante, su efectividad dependerá de la exhaustividad con la que aborde las distintas facetas del tratamiento de datos, garantizando así una protección integral de la privacidad y los derechos fundamentales de los ciudadanos en un entorno digital en constante evolución. Es importante que la regulación avance hacia una reglamentación más específica, clara y aplicable, que tenga en cuenta los riesgos específicos relacionados con el uso de datos biométricos, para proteger efectivamente los derechos fundamentales de los ciudadanos en un entorno cada vez más digitalizado.

RECOMENDACIONES

- **Control de Constitucionalidad**: Someter la normativa ecuatoriana de protección de datos, en especial sobre datos biométricos, a un control de constitucionalidad riguroso, para asegurar la conformidad con los derechos fundamentales, como el de la privacidad. Las disposiciones que no cumplan con los estándares constitucionales deben ser revisadas y ajustadas para evitar la vulneración de derechos.
- **Resolución Vinculante de la Superintendencia:** La Superintendencia de Protección de Datos Personales debe emitir una resolución vinculante que obligue a las entidades a implementar políticas internas específicas para el tratamiento de datos biométricos, incluyendo medidas de seguridad y mecanismos de respuesta ante incidentes, con sanciones por incumplimiento.
- **Interpretación Restrictiva de la Normativa:** La legislación sobre protección de datos debe ser interpretada de manera restrictiva en lo referente a datos biométricos, analizando las circunstancias bajo las que da el tratamiento y autorización de datos y priorizando la protección de los derechos individuales y aplicando los principios de proporcionalidad, minimización, transparencia y consentimiento, garantizando que su uso sea estrictamente necesario y adecuadamente protegido.

- **Suscripción de convenios y adopción de normativa europea:** Se recomienda que Ecuador considere adherirse al Convenio 108+ del Consejo de Europa, un instrumento sofisticado que protege a las personas en cuanto al tratamiento de datos personales, el adoptar prácticas, estudios y mecanismos más avanzados en la gestión de datos personales. Es necesario que se inicie con las gestiones necesarias para la suscripción y se realicen actualizaciones a la normativa ecuatoriana en materia de protección de datos para poder lograr la adecuación al reglamento europeo.

- **Implementación de un manual de tratamiento de datos biométricos:** El desarrollo y la implementación de un manual enfocado específicamente en el tratamiento de datos biométricos, dicho instrumento detallaría los procedimientos, precauciones de seguridad y protocolos de gestión necesarios para proteger estos datos altamente sensibles, como el de otros países. Además,

el manual debería ser obligatorio para todas las organizaciones que manejen datos biométricos, lo que garantizaría la transparencia y rigurosidad en el tratamiento de esta información sensible de acuerdo con los principios legales de seguridad, privacidad, consentimiento y proporcionalidad.

REFERENCIAS

Aguirre, Á. (2023). Uso de datos biométricos (biometría) como método para aceptar las políticas de uso de datos personales. Quito: Universidad Hemisferios.

ARATEK. (28 de Febrero de 2023). Obtenido de https://www.aratek.co/es/news/what-is-biometrics-definition-data-types-trends

Badeni, G. (2006). Tratado de derecho constitucional. Tomo II. Buenos Aire, Argentina: La ley.

Barrio, M. (2021). Formación y Evolución de los Derechos Digitales. Ediciones Olejnik.

Castro, I. (2004). Clasificación de las normas constitucionales. Revista Jurídica. Facultad de Jurisprudencia y Ciencias Sociales y Políticas, 57-73. Recuperado de: https://www.revistajuridicaonline.com/wp-content/uploads/2004/01/17_Clasificacion_Normas_Constitucionales.pdf

Cazurro Barahona, V. (2020). Antecedentes y fundamentos del Derecho a la protección de datos. J.M. BOSCH EDITOR.

Consejo de Europa. (28 de Enero de 1981). Convenio 108 sobre Protección de Datos. Obtenido de The Council of Europe: https://www.coe.int/es/web/data-protection/convention108-and-protocol

Consejo de Europa. (2018). Convenio 108+ sobre Protección de Datos Modernizado. Obtenido de The Council of Europe: https://rm.coe.int/convenio-para-la-proteccion-de-las-personas-con-respecto-al-tratamient/1680968478

Constitución de la República del Ecuador (20 de octubre 2008). Asamblea Nacional. Montecristi: Registro Oficial 449.

Corte Constitucional del Ecuador. (8 de Julio de 2020). Sentencia No. 1868-13-EP. Obtenido de http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOicyNzE4ZjljZC1hZjU4LTQxMTItYjBkYi01MjVlYmUwNDU2ZjgucGRmJ30=

Corte Constitucional del Ecuador. (27 de Enero de 2021). Sentencia No. 2064-14-EP/21. Obtenido de http://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcnBldGE6J3RyYW1pdGUnLCB1dWlkOic1MDM5NmI5Ny1hZmFiLTQ1OWEtYWRlMC1jNjdmNzM1NTMzYjAucGRmJ30=

Cubillos Vélez, Á. (2017). La explotación de los datos personales por los gigantes de internet. Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, 27-55. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=7399685

ECIJA. (21 de septiembre 2022). Biometría y protección de datos personales en el marco de la legislación ecuatoriana. Recuperado de: https://ecija.com/sala-de-prensa/ecuador-biometria-y-proteccion-de-datos-personales-en-el-marco-de-la-legislacion-ecuatoriana/

Guerrero, E. (2022). Uso de tecnologías de reconocimiento facial y sus límites legales en Ecuador. Recuperado de: https://issuu.com/efrenguerrero/docs/reconocimiento_facial_en_ecuador_versi_n_final_00

González, A. G. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. Boletín mexicano de derecho comparado, 40(120),743-778. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332007000300003&lng=es&tlng=es

Hernández, J. M. (2023). ¿Por qué debemos proteger la privacidad?. Cronología, textos y notas sobre intimidad, vida privada y protección de datos. J. M. BOSCH EDITOR.

Instituto Nacional De Transparencia, Acceso a La Información Y Protección De Datos Personales. (2018). Guía Para El Tratamiento De Datos Biométricos. México: INAI.

Ley Orgánica de Protección de Datos Personales. (26 de Mayo de 2021). Asamblea Nacional . Quito: Registro Oficial Suplemento 459.

https://www.fielweb.com/Index.aspx?rn=83420&nid=1162059#norma/1162059

Llanos, A. (1944). El Principio De La Autonomía De La Voluntad Y Sus Limitaciones. Chile: Universidad de Chile.

Manili, P. (2019). Manual de derecho constitucional. Buenos Aires, Argentina: Astrea.

Molinaro, D. (4 de Noviembre de 2022). Avast. Obtenido de https://www.avast.com/es-es/c-what-is-biometric-data#:~:text=En%20ciberseguridad%2C%20la%20definici%C3%B3n%20de,y%20el%20control%20de%20acceso.

Organización de los Estado Americanos (OEA). (Diciembre de 31 de 2021). Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Comité Jurídico Interamericano. Obtenido de https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Resolución Nro. 003-NG-DINARP-2022. Norma de funcionamiento del Sistema de Autenticación Única (SAU). (2022, 9 de agosto) Registro Oficial No. 123

Romero Jiménez, G. (1 de julio 2021). RECONOCIMIENTO FACIAL Entre la seguridad y la privacidad. vLex. Abogacía. Consultado el 5 de agosto de 2024.

San Martín, N. (8 de mayo 2021). El de datos biométricos, un padrón que causa desconfianza. Proceso. Consultado el 3 de agosto de 2024.

Stolfi, G. (2018). Teoría Del Negocio Jurídico. Buenos Aires, Argentina: Ediciones Jurídicas Olejnik.

Velásquez, S. (2010). Manual de derecho procesal. Guayaquil, Ecuador: Edino.

Vera Saltos, M. A., & Vivero Andrade, M. B. (2019). ¿Vida Privada O Muerte a La privacidad?: Protección De Datos Personales En La relación Empresa-Cliente En Ecuador. *USFQ Law Review*, 10. Recuperado de: https://revistas.usfq.edu.ec/index.php/lawreview/article/view/1397/1623

Wendehorst, C. y Duller, Y. (2021). Biometric Recognition and Behavioural Detection. Parlamento Europeo. Recuperado de: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf

DECLARACIÓN Y AUTORIZACIÓN

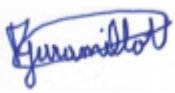
Nosotros, **Jaramillo Navarrete, Romina Damiany**, C.C: # **0956685176**, y **Mora Cuenca, Naomy Carolina**, con C.C: # **0704764323**; autores del trabajo de titulación: **Riesgo en el tratamiento de datos biométricos en servicios digitalizados,** previo a la obtención del título de **ABOGADO** en la 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, a los 30 días del mes de agosto del año 2024

AUTORES



f. _____
Jaramillo Navarrete, Romina Damiany
C.C: **0956685176**

f. _____
Mora Cuenca, Naomy Carolina
C.C: **0704764323**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TEMA Y SUBTEMA:	Riesgo en el tratamiento de datos biométricos en servicios digitalizados		
AUTOR(ES)	Jaramillo Navarrete, Romina Damiany Mora Cuenca, Naomy Carolina		
REVISOR(ES)/TUTOR(ES)	Ab. Cuadros Añazco, Xavier Paul		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia, Ciencias Sociales y Políticas		
CARRERA:	Carrera de Derecho		
TITULO OBTENIDO:	Abogado		
FECHA DE PUBLICACIÓN:	30 de agosto de 2024	No. DE PÁGINAS:	26
ÁREAS TEMÁTICAS:	Protección de datos personales, derecho a la privacidad, Biometría		
PALABRAS CLAVES/ KEYWORDS:	Protección de datos personales, datos biométricos, biometría, seguridad, información, datos sensibles, tecnología, digitalización, consentimiento.		
RESUMEN/ABSTRACT (150-250 palabras): El presente trabajo de investigación tiene como objetivo central analizar la normativa ecuatoriana en materia de protección de datos personales, enfocando el objeto de estudio específicamente en el tratamiento de datos personales biométricos en servicios digitalizados, resaltando la falta de regulación conforme a la biometría y los mecanismos de identificación, reconocimiento, autenticación y seguridad biométricos. Destacamos también, la importancia de una normativa que abarque la protección y manejo de los registros y datos biométricos en la actualidad y contexto ecuatoriano, donde vemos cada día como la era tecnológica y digital abunda más en nuestras vidas, creando nuevas problemáticas para el derecho. Y exponemos posibles soluciones a este problema, que puede parecer reciente, pero su evolución crece de forma acelerada y sin embargo en el ámbito internacional, al menos, cuenta con un extenso desarrollo analítico y normativo el cual consideramos puede ser adoptado por la regulación ecuatoriana, ya que esta aún se mantiene limitada.			
ADJUNTO PDF:	☒ SI	☐ NO	
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-939026057; +593-992991256	E-mail: **rominajaramillonavarrete@gmail.com**; **naomicarolina3@hotmail.com**	
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre: Reynoso Gaute, Maritza Ginette**		
	Teléfono: +593-4-3804600		
	E-mail: maritza.reynoso@cu.ucsg.edu.ec		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			