



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y
POLÍTICAS
CARRERA DE DERECHO**

TEMA:

Consentimiento del trabajador en el tratamiento de Datos Biométricos
mediante la Huella Digital

AUTORES:

Chevasco Murillo, Maria Leonor
Plaza Martinez, Xavier Alejandro

**Trabajo de titulación previo a la obtención del título de
Abogada/o**

TUTOR:

Ab. Cuadros Añazco, Xavier Paul, Mgs

Guayaquil, Ecuador

28 de agosto del 2025



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y
POLÍTICAS
CARRERA DERECHO**

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por
Chevasco Murillo, Maria Leonor y Plaza Martinez, Xavier Alejandro, como
requerimiento para la obtención del título de **abogado/a**.

TUTOR

f. _____

Ab. Cuadros Añazco, Xavier Paul, Mgs.

DIRECTOR DE LA CARRERA

f. _____

Dra. Pérez Puig-Mir, Nuria, PhD.

Guayaquil, a los 28 del mes de agosto del año 2025



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE JURISPRUDENCIA
CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, **Chevasco Murillo, Maria Leonor**
Plaza Martinez, Xavier Alejandro

DECLARAMOS QUE:

El Trabajo de Titulación, **Consentimiento del trabajador en el tratamiento de Datos Biométricos mediante la Huella Digital** 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 28 del mes de agosto del año 2025

LOS AUTORES

f. _____
Chevasco Murillo, Maria Leonor

f. _____
Plaza Martinez, Xavier Alejandro



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y
POLÍTICAS
CARRERA DE DERECHO**

AUTORIZACIÓN

Nosotros, **Chevasco Murillo, Maria Leonor**
Plaza Martinez, Xavier Alejandro

Autorizamos a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Consentimiento del trabajador en el tratamiento de Datos Biométricos mediante la Huella Digital**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y total autoría.

Guayaquil, a los 28 del mes de agosto del año 2025

LOS AUTORES

f. _____
Chevasco Murillo, Maria Leonor

f. _____
Plaza Martinez, Xavier Alejandro



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

TRIBUNAL DE SUSTENTACIÓN

f. _____

MGS. ZAVALA EGAS, LEOPOLDO XAVIER
DECANO O DIRECTOR DE CARRERA

f. _____

Ab. REYNOSO GAUTE, MARITZA GINETTE, Mgs.
COORDINADOR DEL ÁREA

f. _____

DR. AGUIRRE VALDEZ, JAVIER EDUARDO
OPONENTE



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y
POLÍTICAS
CARRERA DE DERECHO**

REPORTE COMPILATIO



f. _____

Chevasco Murillo, Maria Leonor
AUTORA

f. _____

Plaza Martinez, Xavier Alejandro
AUTOR

f. _____

Ab. Cuadros Añazco, Xavier Paul, Mgs.
TUTOR

AGRADECIMIENTO

A Dios, por su guía y fortaleza en cada paso de mi carrera y de mi vida.

A mi madre, Sue Murillo, quien me inspiró y me alentó en cada paso que di; ha sido uno de mis pilares fundamentales y la persona más importante para mí, ejemplo de fortaleza, resiliencia, dedicación, apoyo y, sobre todo, amor. Me ha enseñado a nunca rendirme y a seguir adelante siempre, aunque haya obstáculos, y a ser una mejor versión de mí cada día.

A toda mi familia, que siempre estuvo para mí, apoyándome y sintiéndose orgullosos de la persona en la que me he convertido, dándome ese amor incondicional desde el primer momento.

A mis mejores amigas, Adriana, Karen, Ruth y Janeth, quienes han visto cómo he ido evolucionando como persona y me han acompañado en cada etapa de mi vida.

A mi compañero de tesis, Xavier, quien, a lo largo de toda la carrera, me ha brindado un gran apoyo incondicional. Me siento afortunada de haberlo elegido a él para acompañarme en este maravilloso proceso. Gracias por siempre escucharme, por tu paciencia y por estar en los buenos y malos momentos; por tu confianza, cariño y comprensión. No sé qué habría hecho sin ti durante estos cuatro años de carrera..

A mis amigos más cercanos, que la carrera me ha regalado, porque no sé qué hubiera hecho sin ustedes. Hicieron que este camino fuera más corto y divertido. He vivido experiencias con ustedes que, sin duda, guardaré siempre.

Al resto de mis verdaderos amigos, que la vida me ha regalado, gracias por acompañarme en una aventura más y por estar siempre para mí.

A mi tutor, por su paciencia y por orientarnos para realizar un mejor trabajo.

Chevasco Murillo, María Leonor

AGRADECIMIENTO

Quiero comenzar expresando mi más profundo agradecimiento a mis padres, quienes durante todo este tiempo de carrera se han esforzado por darme siempre lo mejor y priorizar mi educación por encima de cualquier otra cosa. Han sido un pilar fundamental en mi vida y, en cada momento de dificultad, han estado presentes para aconsejarme y escucharme cuando más lo he necesitado.

También deseo agradecer con todo mi corazón a mis abuelos, tanto maternos como paternos, quienes siempre me han mostrado con su ejemplo lo importante que es esforzarse en la vida para alcanzar nuestros sueños. Sus palabras y enseñanzas han sido un faro constante de motivación para lograr lo que ellos tanto ansiaron en sus vidas.

De manera muy especial, quiero agradecer a mi compañera de tesis, quien ha estado a mi lado en este proceso académico. Una persona dedicada y estudiosa, que siempre ha mostrado preocupación por mí y por todo lo que nos rodea. Su apoyo, constancia han sido determinantes para la culminación de este trabajo.

Asimismo, expreso mi sincero agradecimiento al Dr. Xavier Cuadros, quien siempre estuvo presente para orientarnos con sus consejos, apoyarnos en cada momento hasta el último día, brindarnos su ayuda para que este trabajo pudiera culminar con éxito.

Me encantaría poder nombrar a todas las personas que han estado presentes durante este recorrido en la hermosa carrera de Derecho, pero el espacio no sería suficiente. A cada una de ellas les guardo un agradecimiento sincero por su compañía y aportes en este camino.

Finalmente, agradezco a Dios por haber puesto en mi vida a las personas correctas en el momento indicado, por enseñarme y guiarme siempre que lo necesité, y por brindarme la fortaleza para llegar hasta aquí.

Plaza Martinez, Xavier Alejandro

DEDICATORIA

Dedico este trabajo a mi madre, Sue, porque fue ella quien me enseñó a seguir adelante. Nunca dejó de confiar en mí; es una mujer maravillosa y me enorgullece que sea mi madre. Le dedico mi carrera y mi vida, porque sin ella no sería la persona que soy hoy en día. Sin dudarlo, es la mujer en quien algún día aspiro a convertirme.

Se lo dedico, además, a mis hermanos y a mis abuelos, que me acompañan siempre desde el cielo y nunca me han dejado sola; y al resto de personas que me han acompañado durante mi trayectoria y en mi vida.

Y sobre todo le dedico este trabajo a Dios.

Chevasco Murillo, Maria Leonor

Se lo dedico a mis padres Javier Plaza y Martha Martinez quienes siempre han estado ahí para acompañarme en todo este transcurso de tiempo y que yo pueda lograr una de las muchas metas de mi vida, también a mi familiares que cada uno puso un grano de arena para apoyarme siempre pero en especial mis abuelos Héctor y Martha quienes me enseñaron todo lo bueno que soy en la actualidad y que desde pequeño estuvieron para mí, además mi abuela Gioconda quien me cuido siempre y estuvo para mí en mis altas y bajas, estuvo atenta a mí desde mis primeros pasos y siempre me puso antes que nadie para cuidarme a mí y mi abuelo Fernando que siempre me dio el ánimo y las fuerzas para continuar adelante, además también una persona muy especial que ha estado durante todo el transcurso de la carrera apoyándome, estando a mi lado en los buenos momentos y malos, siempre motivándome a ser mejor en todos los ámbitos, alguien el cual me enorgullece haber compartido todo este tiempo a su lado y que espero que sea mucho tiempo más, María Leonor.

También especial de una dedicársela a Dios el cual siempre ha sido mi camino y hay quien me ayuda a tomar las decisiones el cual soy el hombre que soy actualmente.

Plaza Martinez, Xavier Alejandro

ÍNDICE

Contenido

RESUMEN.....	XI
ABSTRACT.....	XII
INTRODUCCIÓN	2
CAPÍTULO I.....	3
1. ANTECEDENTES.....	3
2. DEFINICIONES Y FINALIDAD.....	4
A. LA HUELLA DIGITAL	4
B. EL CONSENTIMIENTO DEL TRABAJADOR	6
C. REQUISITOS DE UN CONSENTIMIENTO VÁLIDO EN LA LOPDP	7
D. DATOS PERSONALES Y DATOS SENSIBLES.....	7
3. PRINCIPIOS (DE PROTECCIÓN DE DATOS PERSONALES).....	8
CAPÍTULO II	12
1. PREGUNTA DE INVESTIGACIÓN	12
2. ANÁLISIS	12
2.1. EL CONSENTIMIENTO EN LA PROTECCIÓN DE DATOS PERSONALES	12
2.2. CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR Y DERECHOS FUNDAMENTALES INVOLUCRADOS	13
2.3. LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPDP) Y SU ÁMBITO LABORAL.....	14
2.4. LEGISLACIÓN COMPARADA	15
2.5. EL CONSENTIMIENTO COMO BASE LEGAL NO EXCLUSIVA EN LA LEY ESPAÑOLA Y ECUATORIANA	17
2.6. JURISPRUDENCIA ESPAÑA	19
CONCLUSIONES	24
RECOMENDACIONES	25
REFERENCIAS.....	28

RESUMEN

En el Ecuador la protección de datos personales ha sido un tema relevante el cual se vino a desarrollar con normativa en mayo del 2021, la promulgación de la Ley Orgánica de Protección de Datos Personales, esto generó en el Ecuador que los empleadores hagan uso de mecanismo de control de asistencias con el uso de los datos biométricos, que en este caso sería la huella digital.

Este trabajo busca analizar el consentimiento de los trabajadores al momento del uso de la huella digital como método de asistencia, además si el consentimiento de los trabajadores podría recaer en una vulneración cuando se trate de otorgar sus datos biométricos como es el caso de la huella digital o si responde a una imposición implícita por parte del empleador y si esta es libre, específico e informado. Mediante un enfoque jurídico y normativo, aplicable en los ámbitos nacionales como internacionales.

El estudio concluye con los vacíos normativos y prácticas empresariales que comprometen a los trabajadores, sugiriendo la necesidad de una regulación más precisa y que cuide los derechos de los trabajadores.

Palabras clave: Datos biométricos, Consentimiento libre, Huella digital, Protección de datos personales, Mecanismos de Control Asistencia, Datos sensibles.

ABSTRACT

In Ecuador, personal data protection has been an important issue, which was addressed in May 2021 with the enactment of the Organic Law on Personal Data Protection. This led employers in Ecuador to use attendance control mechanisms involving biometric data, in this case fingerprints.

This study seeks to analyze workers' consent when using fingerprints as a method of attendance, as well as whether workers' consent could be considered a violation when it comes to providing their biometric data, such as fingerprints, or whether it responds to an implicit imposition by the employer and whether it is free, specific, and informed by using a legal and regulatory approach, applicable at both the national and international levels.

The study concludes with regulatory gaps and business practices that compromise workers, suggesting the need for more precise regulation that protects workers' rights.

Keywords: Biometric Data, Freely Given Consent, Fingerprint, Personal Data Protection, Attendance Control Mechanisms, Sensitive Data.

INTRODUCCIÓN

En el Ecuador en la última década se ha incorporado tecnologías biométricas como una herramienta para tener un control de asistencia de los trabajadores y ciertos usos demás, en esta tesis se hará un análisis acerca de la huella digital y cómo existen alternativas menos intrusivas para evitar su uso entonces esto causa ciertas inquietudes jurídicas en cuanto al consentimiento del trabajador y la protección de sus datos personales. En Ecuador con el lanzamiento de la Ley Orgánica de Protección de Datos Personales deberá ser pertinente analizar y revisar si el consentimiento de los trabajadores es totalmente libre, voluntario e informado o existe un temor reverencial de por medio.

Esta investigación busca un análisis y comprensión más clara de los derechos del trabajador frente a los métodos de uso de los datos sensibles por parte del empleador y se busca generar argumentos y criterios que creen un equilibrio entre los trabajadores y los empleadores.

La investigación acerca del consentimiento de los trabajadores a la hora del uso de su huella dactilar como método de asistencia o ingreso a instalaciones tendrá un enfoque normativo y jurisprudencial, además de una revisión enfocada a un análisis doctrinario complementado con información actualizada de revistas jurídicas en derecho laboral y de datos personales.

DESARROLLO

CAPÍTULO I

1. ANTECEDENTES

El manejo de los datos personales en el Ecuador está transitando un proceso reciente de reconocimiento tanto normativo, institucional y social. La Constitución del Ecuador del 2008 tenía un agregado en el artículo 66, numeral 19 el cual menciona los datos personales del ciudadano como una garantía fundamental. Por otra parte, en el 2021 se promulgó la Ley Orgánica de Protección de Datos Personales en el Ecuador (de ahora en adelante mencionada como LOPDP) tomó posición en delimitar el tratamiento que se le daba a las personas con su información sus datos sensibles. Esta ley fue un gran avance en Ecuador ya que aborda varias problemáticas, sin embargo una ley nueva en la cual había omisiones por parte de nuestra legislación, pero en el ámbito internacional el marco legal de protección de datos ya tenía décadas de existencia y se venía usando y ejecutando desde 1970 en ciertos países Europeos como Alemania, Suecia y Francia, pero Ecuador tomo este marco normativo en el año 2021 buscando su incorporación en la normativa nacional estando varias décadas atrasados y en virtud de compromisos internacionales era cada vez una preocupación social creciente por los riesgos que vive actualmente el Ecuador con la inseguridad al trato de nuestros datos y más aún cuando existe una vulnerabilidad presente con la filtración de información personal y no regulación de esta.

La Superintendencia de Protección de Datos Personales es una entidad nueva en el Ecuador que fue creada en mayo de 2021, a partir de la implementación de la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial Suplemento N.º 459. El motivo el cual Ecuador integro esta normativo fue para asegurar que, cuando una institución pública o privada maneje datos personales, lo haga respetando los derechos de las personas. Además, más allá de su papel sancionador, también busca orientar y promover buenas prácticas, de forma que la protección de la información no sea solo un requisito legal, sino una costumbre dentro de las organizaciones del Ecuador.

En el ámbito el uso de tecnologías biométricas como el registro de asistencia mediante la huella digital se convierte en una práctica regular y común en instituciones públicas y privadas, , sin que exista un análisis crítico sobre su legitimidad ya que esto

hacía propenso a vulneración de datos personales en este caso la huella digital el cual es de uso personalísimo y que existe este uso de registro de asistencia, cuando se puede el empleador implementar uso de otros métodos como tarjetas magnéticas personalizadas, registro manual u otras de alternativas adecuadas, sin necesidad del uso de la huella digital.

La huella digital como dato biométrico en el cual la única finalidad no es solo identificar a una persona tiene una característica que no es reversible, ya que no puede ser cambiada, sustituida ni eliminada. Por eso, su uso de forma irresponsable, como en el control de asistencia laboral, no es correcto si no existe una base válida y un consentimiento claro y sin garantías de fondo técnicas adecuadas para proteger y prevenir algún error o filtración de fondo.

2. DEFINICIONES Y FINALIDAD.

A. LA HUELLA DIGITAL

La huella digital se considera un dato biométrico utilizado para la identificación de manera única a una persona. Esto se puede ver en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea que define a los datos biométricos en su Artículo 3 en el literal 18 como: « «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específicos, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos (Reglamento (UE) 2018/1725 del parlamento Europeo y del Consejo, 2018).

Con lo mencionado anteriormente, los datos dactiloscópicos se refieren solamente a las huellas digitales, reconociéndose jurídicamente como un identificador único e irremplazable que tiene cada persona en el mundo, no existe otra parecida o igual a la que tiene cada uno.

La huella digital con dato biométrico en el ámbito laboral en el Ecuador ha sido objeto de atención por parte de las autoridades de control de datos personales, por el motivo que en el Ecuador, la huella digital se emplea

habitualmente en el ámbito laboral para el control de asistencia de los trabajadores, registrando sus horas de ingreso y salida del personal en sus jornadas laborales, pero esta práctica lo que busca otros medios para el control de asistencias que no requieran la huella digital, pero la implementación de este método con uso de la huella digital genera inconformidad respecto al derecho de protección de datos personales por el motivo que el trabajador no se encuentra en condiciones para negar su autorización del uso de la huella digital como método de registro de asistencia es impuesto como el mecanismo preferencial del empleador para registrar las jornadas de los trabajadores, sin ofrecer o garantizar otros medios menos dañinos para el titular.

En Ecuador, en el entorno laboral, la huella digital tiene como finalidad por parte del empleador gestionar los registros de asistencia, motivó el cual puede hacerse un cambio y buscar alternativas el cual cuiden de mejor manera los derechos personales de los ciudadanos, en este caso los trabajadores por este motivo la protección de los datos personales haciendo énfasis en los biométricos como la huella dactilar tiene un rango constitucional según el Artículo 66 literal 19 de la Constitución de la República del Ecuador el cual dice Art. 66.- Se reconoce y garantizará a las personas 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.(Constitución de la Republica del Ecuador, 2008)

La LOPDP se pronuncia a los datos biométricos como datos personales de categoría especial por el cual su tratamiento está basado en restricciones estrictas, por lo cual, la ley prohíbe tratar datos sensibles salvo en el caso que se cumplan ciertos requisitos explícitos en el ordenamiento jurídico. Entre estas excepciones se encuentran en el Artículo 26 de la LOPDP: 1) el consentimiento explícito del titular otorgado con debidas garantías, y b) el tratamiento necesario para el cumplimiento de obligaciones y ejercicio de derechos del responsable en el ámbito del derecho laboral (Ley Orgánica de Protección de Datos Personales, 2021).

Por otra parte, es de suma importancia destacar que en el Código del trabajo en Ecuador no existe una norma que obligue o autorice el uso de sistemas biométricos para el control de asistencia laboral y si bien el Código del trabajo exige llevar un control adecuado de las asistencias de los trabajadores, sin embargo, no impone ningún método o forma específica para registrar la asistencia de la jornada laboral. Por otra parte, la LOPDP exige en un mandato legal expreso como base de legitimación si se pretende tratar datos sensibles sin consentimiento, entonces en ausencia de tal disposición el empleador no se puede poner en una posición de obligación legal para usar la huella digital de sus empleados.

En Ecuador la Superintendencia de Protección de Datos Personales han empezado a pronunciarse sobre este tipo de prácticas como el uso de huella digital en mecanismo de control de asistencias por parte del empleador, como se puede ver en el Oficio No. IRD-2025-0031-O, que ha mencionado que el uso de la huella digital como mecanismo para registro de asistencia, cuando no cumple con los estándares que se exigen en la LOPDP por el cual el trabajador no tiene una opción real en el cual el consienta o rechace dicho uso de su huella digital para el uso de registro de asistencia en el horario laboral.

B. EL CONSENTIMIENTO DEL TRABAJADOR

El consentimiento del trabajador tiene un papel central al evaluar el uso de datos biométricos en el ámbito laboral, considerando que el registro de asistencia mediante huella digital o mecanismos biométricos es algo frecuente y normalizado. Aunque el uso de estos mecanismos ha sido común y aparentemente normalizado desde inicios del 2010 es de suma importancia por el hecho que hasta el 2021, no existía un marco legal específico que regule el tratamiento de los datos personales y datos sensibles

El tratamiento de la huella digital en el ámbito laboral, durante mucho tiempo, careció de controles efectivos y de criterios claros sobre su legalidad, lo que generaba un riesgo real de vulneración de derechos fundamentales. En este sentido, el consentimiento que brinda el trabajador para utilizar su huella dactilar no puede considerarse totalmente válido, ya que existe un desequilibrio en la relación laboral. Esto ocurre sobre todo cuando la entrega de dicho

consentimiento se convierte en un requisito obligatorio para el desempeño de sus funciones. De esta manera, se evidencia la presencia de un temor reverencial que restringe la libertad del trabajador de negarse.

C. REQUISITOS DE UN CONSENTIMIENTO VÁLIDO EN LA LOPDP

La LOPDP establece que el consentimiento debe cumplir con condiciones para ser valido es decir el consentimiento del titular de datos personales deber ser:

1. Libre
2. Específico
3. Informado
4. Inequívoco

La LOPDP obliga al responsable del tratamiento a poder demostrar que obtuvo dicho consentimiento valido mediante registros verificables el cual pueden ser formularios físicos firmados, contratos, consentimientos electrónicos registrados, registros de sistemas informáticos y más.

D. DATOS PERSONALES Y DATOS SENSIBLES

Por lo principal, los datos personales sensibles se consideran a datos más privado o reservado de una persona natural, a lo que hacemos referencia a datos como la huella digital, entre otros; estos datos son únicos e irrepetible, que conlleva a identificar o reconocer a una persona. Por lo cual, requiere una mayor protección ya que puede ser usado para vulnerar los datos personales de una persona, por lo mismo se necesita que se brinde el consentimiento para el uso de estos datos tan privados, importantes y personales, que pueden ser vulnerados cuando se brinda el consentimiento para un mal uso.

Según la Ley Orgánica de Protección de Datos Personales, los define como:
Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente. [.....] Datos sensibles: Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o

puedan atentar contra los derechos y libertades fundamentales.(Ley Orgánica de Protección de Datos Personales, 2021)

Asimismo, es de importancia destacar que la huella digital suele almacenar en sistemas informáticos mediante plantillas biométricas de cada trabajador en el ámbito laboral. Desde el punto de vista jurídico, las huellas digitales son datos biométricos de extrema importancia ya que son únicos por cada persona existente e irremplazable y el autor Mercader Uguina menciona: la huella dactilar completa identifica completamente a la persona, también es susceptible de identificarse a la misma persona con la toma de muestras o minucias recogidas de partes de la huella y transformadas en una plantilla, aunque sea a través de un algoritmo. (Mercader Uguina, J. R., 2024, p. 13)

Además, es importante destacar que la huella dactilar, en formato digital, suele almacenarse en sistemas informáticos mediante plantillas biométricas de cada trabajador en el ámbito laboral. Una plantilla biométrica es un conjunto de características biométricas que pueden ser usadas para hacer una comparación directa. Desde el punto de vista jurídico, las huellas dactilares son datos biométricos de extrema importancia, ya que son únicas para cada persona existente.

Por otro lado, es importante destacar que la huella digital, en formato digital, suele almacenarse en sistemas informáticos mediante plantillas biométricas de cada trabajador en el ámbito laboral. De acuerdo al libro El uso de la biometría en la prestación de servicios sociales nos menciona: Una plantilla biométrica es un conjunto de características biométricas que pueden ser usadas para hacer una comparación directa (Javier Preciozzi, 2022, p. 15). Desde el punto de vista jurídico, las huellas digitales son datos biométricos de extrema importancia, ya que son únicas para cada persona existente.

3. PRINCIPIOS (DE PROTECCIÓN DE DATOS PERSONALES)

Según el Reglamento General de Protección de Datos de España nos señala los siguientes principios sobre el tratamiento de datos personales jurídicos los cuales son:

Principio de licitud, transparencia y lealtad, que consiste en que los datos deben ser tratados de manera lícita, leal y transparente para el interesado;

Principio de finalidad que implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines;

Principio de minimización de datos, es decir, aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad;

Principio de exactitud, que obliga a los responsables a disponer de medidas razonables para que los datos se encuentren actualizados, se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan;

Principio de limitación del plazo de conservación que constituye una de las materializaciones del principio de minimización. La conservación de esos datos debe limitarse en el tiempo al logro de los fines que persigue el tratamiento. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados, bloqueados o, en su defecto, anonimizados, es decir, desprovistos de todo elemento que permita identificar a los interesados;

Principio de seguridad que impone a quienes tratan datos el necesario análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten;

Principio de responsabilidad activa o responsabilidad demostrada que obliga a los responsables a mantener diligencia debida de manera permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados en base a un análisis de los riesgos que el tratamiento representa para esos derechos y libertades, de modo que el responsable pueda, tanto garantizar como estar en condiciones de

demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.(Principios, 2023)

Estos principios son fundamentales para el tratamiento de datos personas y nos ayudan de forma estructural en el ordenamiento jurídico, además, contribuye de manera interpretativa e integración al sistema jurídico, lo cual fomenta un correcto procedimiento de la información personal.

Calidad: el encargado de dicha información debe pretender tomar las medidas necesarias para eliminar o rectificar datos incorrectos o inequívoco.

Responsabilidad proactiva y demostrada: De acuerdo con el artículo 37 LOPD, los encargados y responsables del tratamiento de estos datos tiene que tomar medidas de seguridad para que dicha información que se reposa en sistemas informativos no sea atacada por personas que quieran vulnerar dicha información, es decir, deben de implementar sistemas de seguridad de la información, garantizado su protección.

Confidencialidad: el responsable debe preservar la protección de los datos en contra de cualquier persona externa que no deba contener dicha información y asimismo, debe imponer medidas que garanticen la confidencialidad de los datos.

Transparencia: Hace referencia que la información de estos datos personales debe ser fácilmente accesible y fácil de entender. La transparencia está sujeta a la lealtad, pues el titular, debe de conocer sobre el uso de sus datos, es decir, debe ser un consentimiento informado. Por lo cual debe ser libre, específico, inequívoco e informado.

Finalidad: El tratamiento se basa en que debe ser determinadas, explícitas, legítimas y comunicadas al titular, por lo cual no podrán tratarse sus datos personales para fines distintos para que fuesen solicitados.

Para finalizar el primer capítulo, se estableció las bases conceptuales y normativas para la revisión y análisis del tratamiento de datos biométricos sensibles

en el ámbito laboral además se menciona que el uso de huella digital como mecanismo de control de asistencia no está basado por una obligación jurídica específica, y que su implementación debe ser evaluada bajo los principios de proporcionalidad, minimización y finalidad. También se puede verificar que en relaciones de subordinación es decir el empleado con el trabajador el consentimiento es difícilmente que se pueda considerar libre y voluntario para el motivo de este temor reverencial y estos resultados respaldan la necesidad de revisar y fortalecer la normativa vigente, promoviendo alternativas que garanticen de forma correcta la protección de los derechos de las personas.

CAPÍTULO II

1. PREGUNTA DE INVESTIGACIÓN

De acuerdo con nuestro análisis, planteamos como un problema jurídico: ¿El consentimiento del trabajador constituye como base legítima para el tratamiento de sus datos biométricos?

2. ANÁLISIS

2.1. EL CONSENTIMIENTO EN LA PROTECCIÓN DE DATOS PERSONALES

En primer punto a analizar, es la Sentencia No. 2064-14-EP/21 de la Corte Constitucional, donde señala que: este tipo de manifestación de voluntad, esta requiere ser libre, específica, informada e inequívoca. Por consiguiente, que aquella sea libre, implica que la misma no esté sujeta a algún tipo de vicio del consentimiento, como la fuerza, la coerción o cualquier tipo de presión que se pueda ejercer sobre el titular, con el fin de que aquel preste su consentimiento. El requisito de especificidad implica que haya claridad en cuanto al tipo de tratamiento que autoriza el titular y el dato personal sobre el cual lo autoriza, así como a los sujetos que pueden realizar el tratamiento sobre los datos personales. Es decir, que la manifestación de voluntad exprese concretamente el o los tipos de tratamiento que se autorizan y específicamente con respecto a qué dato personal del titular se está autorizando dicho uso, así como el sujeto o los sujetos autorizados a realizar dicho tratamiento a los datos personales del titular. En cuanto al requisito de que el consentimiento sea inequívoco, ello está vinculado a la especificidad y claridad e implica que la manifestación de voluntad no sea ambigua, esto es, que no dé lugar a dudas respecto del consentimiento en sí mismo y su alcance. (Sentencia No. 2064-14-EP/21, 2021, p. 28)

Determino que dicho consentimiento debe de ser libre, específico, informado e inequívoco, por lo que al ser un consentimiento libre no debería recaer a algún tipo de presión para que brinde el consentimiento el titular del dato personal. En este sentido, en el ámbito laboral, lo que se pretende enfatizar es que, cuando un trabajador accede a un puesto de trabajo, junto con el contrato laboral, se le solicita la firma de un acta mediante la cual otorga su autorización al empleador para el uso de sus datos personales, como la huella digital, con el fin de registrar su asistencia. Por lo cual

estaría recayendo a un vicio del consentimiento del trabajador porque si el trabajador no acepta el acceso a su dato de la huella digital, le negaran la oportunidad de trabajo.

En la rama del derecho de protección de datos, el consentimiento del titular se reconoce como una de las bases fundamentales para el tratamiento de información personal como es en este caso, la huella digital. Asimismo, es de suma importancia recalcar que basar un tratamiento de datos personales exclusivamente en el consentimiento del titular, podría derivar en un tratamiento inadecuado por parte del titular o cualquier persona que pueda acceder a ella.

Por otra parte, aunque la normativa ecuatoriana, en concordancia con estándares internacionales exige que el consentimiento no solo exista formalmente dictado en un contrato, sino que este cumpla con los requisitos de validez. En particular, uno de los requisitos del consentimiento que deseamos puntualizar es que dicho consentimiento sea libre, sin ninguna coacción, sin engaño y sin que exista una posición de poder en el cual vicie la voluntad del titular, en este caso el trabajador. En palabras de la LOPDP, el consentimiento es válido si es autónomo, confiable, específico e irrefutable, lo cual implica ausencia de presiones indebidas.

2.2. CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR Y DERECHOS FUNDAMENTALES INVOLUCRADOS

La Constitución de la República del Ecuador consagra el derecho a la protección de datos personales de manera clara y expresa en el Artículo 66, numeral 19 donde nos menciona: Art. 66.- Se reconoce y garantizará a las personas: el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección (Constitución de la Republica del Ecuador, 2008).

La norma constitucional establece dos premisas fundamentales en relación con el manejo de los datos personales el cual establece decidir sobre el uso de sus datos y la autorización expresa del titular sobre este. Entonces desde el nivel más alto del ordenamiento jurídico ecuatoriano se establece que el tratamiento de datos personales incluidos los datos biométricos solo serán lícitos si cuenta con el consentimiento del afectado o con una habilitación legal específica.

En consecuencia, el marco constitucional ecuatoriano estipula que el tratamiento de datos personales, incluidos los datos biométricos como la huella digital, será legítimo únicamente si cuenta con el consentimiento del titular o con una habilitación legal específica. Sin embargo, en el ámbito laboral, esta relación de subordinación entre empleador y empleado podría recaer en un temor reverencial que generar un desequilibrio que afecte la libre voluntad del trabajador, haciendo que el consentimiento otorgado pueda no ser plenamente libre ni voluntario.

Por lo tanto, aunque nuestra Constitución reconoce el consentimiento como base para el tratamiento de datos, en el ámbito laboral se debe considerar que este consentimiento podría no ser una base legítima por sí sola, por lo cual si pudiera ser una base legítima el contrato de trabajo el cual disponga otros medios para el registro de asistencia que no sea la utilización de datos biométricos, que si afectan al titular de estos datos sensible. Es fundamental evaluar si existen alternativas menos intrusivas que garanticen una protección de datos adecuada para el trabajador.

2.3. LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES (LOPD) Y SU ÁMBITO LABORAL

En primer término, es preciso considerar lo que se ha desarrollado dentro nuestra legislación de acuerdo a la LOPDP nos menciona que: Art. 7.-Tratamiento legítimo de datos personales.-El tratamiento será legítimo y lícito si se cumple con alguna de las siguientes condiciones: 1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades específicas (Ley Orgánica de Protección de Datos Personales, 2021); donde se analiza que dicho tratamiento del uso de los datos personales como uso de la huella digital u otros datos biométricos, se requiere del consentimiento del trabajador para su uso legítimo. Además, dentro del presente artículo señalado no hace alusión a un uso específico del cual se va a dar la autorización para su tratamiento, por lo cual se da la posibilidad de un mal tratamiento del dato personal sensible.

La LOPDP menciona en el artículo ya analizado, donde enumera las bases que se debe de cumplir para el tratamiento de datos personales entre estos figuran: el

consentimiento del titular; el cumplimiento de una obligación legal; el cumplimiento de una orden judicial; el ejercicio de funciones públicas; la ejecución de un contrato con el titular; la protección de intereses vitales; el tratamiento de datos provenientes de fuentes de acceso público; y el interés legítimo del responsable.

Para el caso de datos sensibles esta tiene una regla especial el cual es que está prohibido tratarlos salvo ciertas circunstancias excepcionales que están señaladas en la LOPDP, dentro del Artículo 25 de la presente ley, se categoriza como datos personales como un dato sensible, es decir, la huella digital al ser un dato biométrico único tiene una protección reforzada

Asimismo, en el Artículo 26 de la misma ley nos menciona las prohibiciones para el tratamiento de datos personales sensibles. No obstante, nos menciona las excepciones para su tratamiento, dentro del literal A, hace alusión a que el titular de este dato personales sensible debe de dar su consentimiento bajo fines específicos, sin embargo, la presente ley no establece de manera expresa los fines para el tratamiento de dichos datos, lo que podría derivar en un tratamiento inadecuado al no especificarse claramente sus finalidades. Por otro lado, en el literal B, hace una mención más específica, a manera de excepción, en la que dicho tratamiento resulte necesario para el cumplimiento de obligaciones y derechos específicos en el ámbito laboral, de seguridad y protección social. Esto implica que se permite el uso de datos personales sensibles cuando su finalidad sea el cumplimiento de dichas obligaciones, lo que conllevaría a que el trabajador proporcione su dato personal sensible para el cumplimiento de obligaciones laborales.

2.4. LEGISLACIÓN COMPARADA

Hoy en día en el Ecuador el uso de los datos biométricos como la huella digital en el entorno laboral ha generado algunos desafíos legales en la materia de protección de datos personales, en particular surge el inconveniente si el consentimiento del trabajador puede considerarse una base legítima en este tipo de datos sensibles. En base a lo tratado se analizará y compara con el marco normativo de España y Ecuador sobre el tratamiento de datos biométricos en el ámbito laboral poniendo relevancia en el rol del consentimiento. Este enfoque de legislación comparada permitirá evidenciar similitudes y diferencias entre ambos marcos

legales, y demostrar por que el consentimiento en una relación laboral no constituye una base legítima para el tratamiento.

El marco normativo en España en materia de protección de datos personales es ampliamente reconocido por su solidez y evolución histórica. España fue uno de los primeros países de la Unión Europea en preocuparse por regular de manera específica la protección de datos personales. Su punto de partida estuvo en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), que sentó las bases de lo que hoy se entiende como la normativa moderna en la materia. Con el paso de los años, este marco se armonizó con el Reglamento (UE) 2016/679, conocido como Reglamento General de Protección de Datos (RGPD), y más tarde se reforzó a nivel interno con la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Actualmente, la legislación española no se limita a reproducir lo dispuesto en el RGPD, sino que lo complementa con disposiciones adaptadas a su propia realidad jurídica. Entre ellas destacan normas específicas para el tratamiento de categorías sensibles, como los datos biométricos, además de un énfasis en principios como la proporcionalidad, la necesidad y la minimización en el ámbito laboral.

En contraste, el Ecuador ha desarrollado su marco legal de protección de datos personales recientemente, es necesario hacer mención que la Constitución de la República del Ecuador del 2008 hace mención del derecho de protección de datos personales, pero en el marco normativo en el Ecuador desde mayo del 2021 se promulgó la LOPDP. Por otro lado, es de importancia mencionar que el marco normativo ecuatoriano en protección de datos personales busca alinearse con el estándar europeo adaptando muchos principios y conceptos del RGPD. No obstante, nuestra LOPDP es una legislación muy reciente cuyo cumplimiento de adaptación nacional e implantación aún está en desarrollo, pese a ello al ser una normativa reciente su aplicación práctica y desarrollo aún se encuentra en una fase inicial por lo cual con el avance normativo y jurisprudencial se podrá igualar o superar la normativa europea.

2.5. EL CONSENTIMIENTO COMO BASE LEGAL NO EXCLUSIVA EN LA LEY ESPAÑOLA Y ECUATORIANA

Por otra parte, dentro de la legislación de España tiene aspectos más avanzado el cual es en reconocer que el consentimiento del titular de los datos no es la única ni necesariamente la principal base legal para el tratamiento de datos personales. Tanto el Reglamento (UE) 2016/679, RGPD, como la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, establecen múltiples bases de legitimación.

En particular, el Artículo 5 del RGPD europeo el cual hace mención de cinco literales donde se pronuncia las bases jurídicas para tratar datos personales son:

Artículo 5.- Licitud del tratamiento. - El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

- a) el tratamiento es necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de potestades publicas conferidas a las instituciones y organismos de la Unión;
- b) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- c) el tratamiento es necesario para el cumplimiento de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
- d) el interesado ha prestado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- e) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física. (Reglamento (UE) 2018/1725 del parlamento Europeo y del Consejo, 2018)

En la normativa de España y de la Unión Europea acerca de la protección de datos, el consentimiento no constituye el único fundamento jurídico para el tratamiento de datos, pues se reconocen otras bases de también válidas. El Reglamento General de Protección de Datos mantuvo este enfoque en un conjunto de fundamentos alternativos. La práctica española ha puesto de relieve que, en determinados ámbitos,

el consentimiento puede resultar inadecuado o insuficiente; por ejemplo, en las relaciones laborales, no se considera válido el consentimiento otorgado por el trabajador al empleador debido al temor reverencial que tiene el empleador con el trabajador. La Agencia Española de Protección de Datos (2023) en tratamientos de datos biométricos menciona que el alto riesgo, como los biométricos en esencial huella dactilar o iris para control laboral, el consentimiento no puede levantar la prohibición ni servir de base de licitud, dado que la relación asimétrica impide garantizar una verdadera libertad de decisión.

En estos casos, deben emplearse otras alternativas menos corrosivas en el ámbito laboral como control de asistencia por tarjeta magnética, aplicaciones móviles, pin personal, Código QR y más.

En Ecuador, si bien durante mucho tiempo el consentimiento fue visto como el eje central y necesario para el tratamiento de datos personales, con la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP) en mayo de 2021 se adoptó una visión más amplia y acorde con los estándares europeos. En su artículo 7, la normativa dispone que el tratamiento de datos se considera legítimo siempre que exista al menos una de las siguientes bases: el consentimiento del titular, que debe ser libre, específico, informado e inequívoco; el cumplimiento de una obligación legal; una orden judicial; una misión de interés público; la ejecución de obligaciones contractuales o medidas precontractuales; la protección de intereses vitales; el uso de información proveniente de fuentes de acceso público o, finalmente, la satisfacción de un interés legítimo por parte del responsable o de un tercero, siempre que no se vulneren los derechos fundamentales del titular.

Esta evolución demuestra que Ecuador ha dejado de fundamentar exclusivamente la licitud del tratamiento en el consentimiento, reconociendo, como España, un catálogo de bases legales alternativas. Pero la principal diferencia radica en el tipo de desarrollo de cada legislación ya que mientras España cuenta con muchos años de experiencia y pronunciamientos de materia de datos personales Ecuador apenas comienza este proceso. La Superintendencia de Protección de Datos Personales (SPDP) ha resaltado que, en contextos de subordinación como el laboral, es difícil considerar el consentimiento plenamente libre, recomendando priorizar fundamentos jurídicos más sólidos. Esta aproximación refleja la clara influencia del modelo español

y europeo, aunque su aplicación en Ecuador se encuentra en una etapa inicial de consolidación.

2.6. JURISPRUDENCIA ESPAÑA

Para este análisis, conviene tener en cuenta que las decisiones de tribunales de otros países, es decir, la jurisprudencia que es una herramienta útil para ver cómo se interpreta y aplica la norma en su propio ordenamiento jurídico. Aunque esas decisiones no son obligatorias en nuestro país porque no tiene la característica de vinculante, son una buena referencia para conocer cómo otras leyes han tratado el tema, muchas veces con un desarrollo más avanzado en la materia. Asimismo, se tendrá especialmente en cuenta la jurisprudencia de los tribunales de España, país que, como ya se señaló, cuenta con uno de los enfoques más desarrollados sobre la materia de protección de datos personales.

Según lo expuesto en la Expediente N.º: PS/00050/2021, dictada por la Agencia Española De Protección de Datos donde se analizó un caso en el que una empresa utilizada los sistema de registro de asistencia mediante la huella digital, lo que se pretende puntualizar si este sistema es necesario, la Agencia desarrollo que: se ha de acreditar la necesidad del tratamiento de datos a través del registro de huellas y proporcionalidad para el cumplimiento de la obligación legal del registro de jornada. Se considera que pueden existir sistemas alternativos al utilizado que cumplen con los principios de proporcionalidad, necesidad y minimización en el tratamiento de datos.(Expediente nº: PS/00050/2021, 2021, p. 15)

Esto implica que para el tratamiento de este dato personal sensible se requiere demostrar que sea proporcional, necesario y exista una minimización en el tratamiento, es decir, que puedan existir otro medio en el ámbito de trabajo que se pueden implementar que no requiera este tratamiento de la huella digital, como tarjetas magnéticas.

Más adelante se analizó que: Por ello, más que la base jurídica de dicho tratamiento, antes de su inicio se debe realizar una prueba de proporcionalidad con el fin de determinar si el tratamiento es necesario para lograr un fin legítimo, así como

las medidas que deben adoptarse para garantizar que las violaciones de los derechos a la vida privada y al secreto de las comunicaciones se limiten al mínimo. Esto puede formar parte de una evaluación de impacto relativa a la protección de datos (EIPD).(Expediente nº: PS/00050/2021, 2021, p. 16) Por lo cual, se ha señalado que se requiere realizar una prueba de proporcionalidad para que se determine que dicho tratamiento sea necesario, sin que esta sea violatoria de derechos del titular.

De igual forma, la Agencia sostuvo que: Antes de implantar un sistema de reconocimiento de huella dactilar, el responsable debe de valorar si hay otro sistema menos intrusivo con el que se obtenga idéntica finalidad. (Expediente nº: PS/00050/2021, 2021, p. 16) Dicho razonamiento conduce a concluir que, el responsable del tratamiento de datos personales debe de verificar que existan otros medios menos lesivos para titular del dato, con la finalidad de encontrar otro mecanismo que cumpla la misma finalidad que se busca con el sistema del reconocimiento de la huella, como puede ser las tarjetas magnética

Con relación a lo anterior, en el Expediente No: EXP202304834 se analizó: Además de levantar la prohibición sobre su tratamiento, el responsable debe acreditar también que su tratamiento se puede realizar porque concurre una de las bases jurídicas legitimadoras del tratamiento contenidas en el artículo 6.1 del RGPD, que son requisito general para el tratamiento de cualquier dato de carácter personal. Esto es, la concurrencia de una excepción que hipotéticamente permita levantar la prohibición de tratar datos biométricos no será suficiente, no sustituye a la necesidad de que a su vez exista una base de licitud en el caso de los biométricos.(Expediente No: EXP202304834, 2024, p. 21) Por consiguiente, lo que se busca precisar en dicha resolución, toda vez que se permita el uso del tratamiento del dato personal cuando esté prohibido, solamente será permitido cuando cumpla con lo establecido dentro del ordenamiento jurídico por ser un dato de carácter personalísimo e irremplazable se debe de tener el mayor cuidado. Sin embargo, la Agencia Española de Protección de Datos menciona que no basta con cumplir con lo diga el ordenamiento jurídico, sino que además se debe de demostrar la necesidad de que la utilización de este tratamiento debe de ser lícito.

En lo que respecta al análisis que se debe hacer previamente para la utilización de estos datos biométricos como lo es la huella dactilar, la Agencia Española señala: Y ello por cuanto el responsable que pretenda instaurar un tratamiento de datos personales de esta naturaleza ha de asegurarse que se supera lo que se ha denominado en la jurisprudencia “el triple juicio de proporcionalidad”, planteándose en especial si el tratamiento de datos biométricos es necesario, idóneo y proporcional. Si existen otros sistemas no biométricos que permitan conseguir la misma finalidad de identificar-verificar la identidad de las personas con eficacia, no será necesario iniciar tratamientos biométricos, y, por tanto, implantar este sistema se considerará contrario al RGPD. Este juicio debe ser el punto de partida de su análisis, pues sólo en caso de que estos métodos superen el citado triple juicio, se exigirá el cumplimiento de otros requisitos o garantías.(Expediente No: EXP202304834, 2024, p. 28)

En relación con el test de triple juicio de proporcionalidad, la Agencia Española menciona:

En relación con el análisis de la necesidad del tratamiento, destacamos los siguientes aspectos:

a. Juicio de idoneidad En relación al juicio de idoneidad, hay que dilucidar si el tratamiento de datos biométricos es necesario para responder a una necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable, y viniendo determinada dicha idoneidad del tratamiento por su efectividad en minimizar el riesgo para el que se aplica. [...]permite cumplir, con garantías de seguridad, las obligaciones del Colegio de la gestión laboral del control horario de la asistencia [...], por lo que se considera que la medida es idónea. b. Juicio de necesidad En relación al juicio de necesidad, hay que dilucidar la probabilidad de que el tratamiento sea eficaz para responder a la necesidad en cuestión del tratamiento de la huella dactilar para minimizar riesgos de incumplimiento de las obligaciones del Colegio de la gestión laboral del control horario de sus empleados.[...] c. Juicio de proporcionalidad: análisis del balance entre riesgo-beneficio En relación al juicio de proporcionalidad del tratamiento, este viene determinado por la posibilidad de aplicar otras medidas menos intrusivas que puedan proporcionar el mismo grado de efectividad. A tal efecto se ha analizado la aplicación de otras medidas de control horario de los empleados que pudieran minimizar los riesgos para los 28 derechos y libertades de los empleados

utilizando sistemas no biométricos, como por ejemplo el uso de tarjetas o aplicaciones mediante códigos alfanuméricos personales o contraseñas, constatando que estos no asegurarían al Colegio una comprobación fiable de la identificación y autenticación unívoca de los usuarios porque permitirían ser fácilmente intercambiados. [...] (Expediente No: EXP202304834, 2024, pp. 29-30)

En otras palabras, este test nos ayuda para verificar que en el ámbito laboral, el responsable del tratamiento haga un buen uso como son datos biométricos sensible por parte del trabajador, el responsable debe de demostrar que está dentro de estos parámetros para su utilización, para que así no recaiga en una vulneración de derechos.

Para concluir con el análisis con énfasis en el modelo español, europeo y ecuatoriano nos demuestra que como consentimiento para el tratamiento de estos datos personales sensibles como la huella digital se debe de tener un excesivo cuidado por parte del responsable, haciendo hincapié en el ámbito laboral no puede considerarse como una base jurídica valida el consentimiento debido a que existe una relación contractual de dependencia, una influencia jerárquica entre el empleador con el trabajador, es decir, una relación de subordinación que pueden afectar directamente a la libertad de decisión del trabajador, por lo cual, el consentimiento estaba siendo viciado, se estaría vulnerando los derechos de los titular del tratamiento. Asimismo, como se ha destacado en jurisprudencia de la Agencia española, nos señala que el consentimiento no sería libre, cuando el titular del tratamiento no puede decir cómo puede tratárselo, además, demuestra que al ser la huella digital un dato sensible personal, que sería irremplazable y que puede verse afectado por vulneraciones, lo que se busca es la implementación de dispositivos menos lesivos para el trabajador que no requiera dar sus datos personales.

En el presente capítulo se ha destacado que, a nivel internacional, nos señala que previamente de implementar sistemas de control de asistencias basados en tecnologías

biométricas, se requiere realizar una evaluación de necesidad, idoneidad y proporcionalidad la cual verificar que este control de asistencia no sea abusivo, sino que se demuestra su necesidad absoluta, considerando la existencia de alternativas tecnológicas menos invasivas y más respetuosas a la privacidad del trabajador por este motivo hacemos énfasis en el capítulo segundo que la jurisprudencia española sostiene que el consentimiento carece de plena validez si no se brindan opciones reales al trabajador.

Por último, lo que se busca implementar de acuerdo a lo analizado es que se considere para no ser vulneradora de derechos para el titular de los datos personales biométricos, en específico de la huella digital, se brinde la libre escogencia de otro mecanismo menos desfavorable para el trabajador.

CONCLUSIONES

1. Dentro del primer capítulo, se mencionó los antecedentes sobre los Datos Personales, lo cual se busca proteger datos sensibles como la huella digital, cuyo uso en el control de asistencia laboral puede recaer en vulneración de derechos si no existe un consentimiento libre, informado, inequívoco y específico, pues se trata de un dato biométrico único e irreversible que exige altos estándares de seguridad y tratamiento responsable.
2. En este segundo capítulo, en el análisis comparativo y jurídico sobre el tratamiento de datos biométricos, específicamente la huella digital, dentro del ámbito laboral no garantiza por sí solo la protección de los derechos del trabajador debido a la subordinación que existe con el empleador; por ello, para evitar la vulneración de derechos del titular de estos datos, se propone garantizar la libre elección de mecanismos alternativos menos desfavorables que el uso de la huella digital.
3. Por último, de acuerdo con el análisis realizado, se propone que, para no vulnerar los derechos del titular de datos biométricos, en especial de la huella digital, se garantice la opción de utilizar mecanismos alternativos menos lesivos para no vulnerar al trabajador. Además, su uso deberá estar condicionado al consentimiento libre, informado, inequívoco y específico, asegurando que la elección sea libre y consciente; por consiguiente, no solamente debe estar sujeta aquello, sino que también debería hacer el test de proporcionalidad

RECOMENDACIONES

En atención al análisis efectuado, y con la finalidad de impulsar una reforma en relación con las disposiciones actualmente permitidas como resultado de nuestro análisis, llegamos a la conclusión de hacer Reforma de la Ley Orgánica de Protección de Datos Personales del capítulo IV categorías especiales de datos del Artículo 26 de la presente ley.

Artículo Actual

Art. 26.-Tratamiento de datos sensibles. -Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias: a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines. b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social.

Reforma propuesta:

Artículo 26.- Tratamiento de datos personales sensibles.

Se prohíbe el tratamiento de datos personales sensibles, salvo en los supuestos excepcionales expresamente previstos en la ley que habiliten su tratamiento. En todos los casos, el responsable del tratamiento deberá justificar, de manera documentada y verificable, la necesidad y proporcionalidad de su utilización, acreditando que no existen medios o alternativas menos intrusivas y que su implementación resulta imprescindible para alcanzar la finalidad legítima invocada.

El responsable tiene la obligación de garantizar la máxima seguridad, custodia y confidencialidad en el manejo de los datos, con especial cuidado en aquellos considerados de especial protección, como los biométricos, dado el alto nivel de riesgo que representan para los derechos y libertades individuales. En el contexto laboral, el trabajador conserva el derecho inalienable de optar por mecanismos alternativos que resulten menos invasivos para su privacidad, siempre que dichos medios permitan cumplir de manera efectiva con la finalidad legítima establecida. El tratamiento de datos personales sensibles únicamente será admisible en los siguientes casos:

- a) Cuando el titular otorgue su consentimiento explícito, libre, informado y específico, dejando claramente establecida la finalidad para la cual serán tratados sus datos.
- b) Cuando el tratamiento sea indispensable para el cumplimiento de obligaciones o el ejercicio de derechos reconocidos por la ley, en materia laboral, de seguridad o protección social, incluyendo, entre otros, la realización de exámenes médicos de aptitud laboral exigidos por el empleador y la gestión de información de salud para la concesión de prestaciones, seguros o pensiones.
- c) Cuando resulte estrictamente necesario para el cumplimiento de obligaciones o el ejercicio de derechos en los ámbitos laboral, de seguridad social o sanitario, siempre que no exista una alternativa menos lesiva para los derechos del titular.
- d) Cuando, en el ejercicio de funciones públicas, una disposición legal lo disponga de forma expresa y el tratamiento sea estrictamente necesario para la ejecución de dichas funciones.

En el caso que se autorice el tratamiento de datos personales sensibles, la Superintendencia de Protección de Datos Personales deberá realizar un test de

proporcionalidad que permita determinar la legitimidad y adecuación del tratamiento propuesto. Este test evaluará, como mínimo, los siguientes elementos:

1. Idoneidad: Determinar si el tratamiento propuesto es apto y eficaz para alcanzar la finalidad legítima invocada.
2. Necesidad: Verificar que no existan alternativas menos intrusivas que permitan alcanzar la misma finalidad con igual eficacia.
3. Proporcionalidad en sentido estricto: Analizar si los beneficios esperados del tratamiento superan las posibles afectaciones a los derechos y libertades del titular de los datos.

La autorización para proceder con el tratamiento de datos sensibles quedará condicionada a que el responsable supere satisfactoriamente las tres etapas del test y se comprometa a la adopción de medidas técnicas, organizativas y jurídicas que garanticen el más alto estándar de protección de datos, así como la rendición de cuentas permanente ante la autoridad competente.

REFERENCIAS

Constitución de la Republica del Ecuador, Registro Oficial 449 (2008).

https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Expediente No: EXP202304834 (30 de octubre de 2024).

Expediente n°: PS/00050/2021 (Agencia Española de Protección de Datos 19 de

febrero de 2021). [https://docuvelneo.s3.eu-west-](https://docuvelneo.s3.eu-west-1.amazonaws.com/resoluciones/documentos/AEPD_394442.pdf?X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVGTA2W7W6HHR5E7R%2F20250812%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20250812T033957Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-Signature=ad3347f5665283b594fa9a44850363363b9a941b3e6c5f6781fc082edcfe6c46)

[1.amazonaws.com/resoluciones/documentos/AEPD_394442.pdf?X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-](https://docuvelneo.s3.eu-west-1.amazonaws.com/resoluciones/documentos/AEPD_394442.pdf?X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVGTA2W7W6HHR5E7R%2F20250812%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20250812T033957Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-Signature=ad3347f5665283b594fa9a44850363363b9a941b3e6c5f6781fc082edcfe6c46)

[HMAC-SHA256&X-Amz-](https://docuvelneo.s3.eu-west-1.amazonaws.com/resoluciones/documentos/AEPD_394442.pdf?X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVGTA2W7W6HHR5E7R%2F20250812%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20250812T033957Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-Signature=ad3347f5665283b594fa9a44850363363b9a941b3e6c5f6781fc082edcfe6c46)

[Credential=AKIAVGTA2W7W6HHR5E7R%2F20250812%2Feu-west-](https://docuvelneo.s3.eu-west-1.amazonaws.com/resoluciones/documentos/AEPD_394442.pdf?X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVGTA2W7W6HHR5E7R%2F20250812%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20250812T033957Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-Signature=ad3347f5665283b594fa9a44850363363b9a941b3e6c5f6781fc082edcfe6c46)

[1%2Fs3%2Faws4_request&X-Amz-Date=20250812T033957Z&X-Amz-](https://docuvelneo.s3.eu-west-1.amazonaws.com/resoluciones/documentos/AEPD_394442.pdf?X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVGTA2W7W6HHR5E7R%2F20250812%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20250812T033957Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-Signature=ad3347f5665283b594fa9a44850363363b9a941b3e6c5f6781fc082edcfe6c46)

[SignedHeaders=host&X-Amz-Expires=86400&X-Amz-](https://docuvelneo.s3.eu-west-1.amazonaws.com/resoluciones/documentos/AEPD_394442.pdf?X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVGTA2W7W6HHR5E7R%2F20250812%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20250812T033957Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-Signature=ad3347f5665283b594fa9a44850363363b9a941b3e6c5f6781fc082edcfe6c46)

[Signature=ad3347f5665283b594fa9a44850363363b9a941b3e6c5f6781fc082](https://docuvelneo.s3.eu-west-1.amazonaws.com/resoluciones/documentos/AEPD_394442.pdf?X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVGTA2W7W6HHR5E7R%2F20250812%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20250812T033957Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-Signature=ad3347f5665283b594fa9a44850363363b9a941b3e6c5f6781fc082edcfe6c46)

[edcfe6c46](https://docuvelneo.s3.eu-west-1.amazonaws.com/resoluciones/documentos/AEPD_394442.pdf?X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAVGTA2W7W6HHR5E7R%2F20250812%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20250812T033957Z&X-Amz-SignedHeaders=host&X-Amz-Expires=86400&X-Amz-Signature=ad3347f5665283b594fa9a44850363363b9a941b3e6c5f6781fc082edcfe6c46)

Javier Preciozzi. (2022). *El uso de la biometría en la prestación de servicios*

sociales. [https://publications.iadb.org/es/publications/spanish/viewer/El-uso-](https://publications.iadb.org/es/publications/spanish/viewer/El-uso-de-la-biometria-en-la-prestacion-de-servicios-sociales-buenas-practicas.pdf)

[de-la-biometria-en-la-prestacion-de-servicios-sociales-buenas-practicas.pdf](https://publications.iadb.org/es/publications/spanish/viewer/El-uso-de-la-biometria-en-la-prestacion-de-servicios-sociales-buenas-practicas.pdf)

Ley Orgánica de Protección de Datos Personales, Registro Oficial Suplemento 459

(2021). [https://www.finanzaspopulares.gob.ec/wp-](https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf)

[content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.p](https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf)
df

Mercader Uguina, J. R. (2024). *El “Big Bang” de la biometría laboral de la huella*

dactilar a los neurodatos.

Principios. (2023, noviembre 10). Agencia Española de Protección de Datos.

<https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/principios>

Reglamento (UE) 2018/1725 del parlamento Europeo y del Consejo (2018).

Sentencia No. 2064-14-EP/21 (Corte Constitucional del Ecuador 2021).

https://esacc.corteconstitucional.gob.ec/storage/api/v1/10_DWL_FL/e2NhcN

BldGE6J3RyYW1pdGUhLCB1dWlkOic1MDM5NmI5Ny1hZmFiLTQ1OW

EtYWRIMC1jNjdmNzM1NTMzYjAucGRmJ30=



DECLARACIÓN Y AUTORIZACIÓN

Nosotros, **Chevasco Murillo, Maria Leonor y Plaza Martinez, Xavier Alejandro** con C.C: # **0925196503** y **0954220646**; autores del trabajo de titulación: **Consentimiento del trabajador en el tratamiento de Datos Biométricos mediante la Huella Digital** 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, 28 de agosto 2025

f. _____

Chevasco Murillo, Maria Leonor

C.C: 0925196503

f. _____

Plaza Martinez, Xavier Alejandro

C.C: 0954220646

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TEMA Y SUBTEMA:	Consentimiento del trabajador en el tratamiento de Datos Biométricos mediante la Huella Digital		
AUTORES	Chevasco Murillo, Maria Leonor y Plaza Martinez, Xavier Alejandro		
REVISOR/TUTOR	Ab. Cuadros Añazco, Xavier Paul, Mgs.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia, Ciencias Sociales y Políticas		
CARRERA:	Carrera de Derecho		
TÍTULO OBTENIDO:	Abogado de los Tribunales y Juzgados de la Republica del Ecuador		
FECHA DE PUBLICACIÓN:	28 de agosto de 2025	No. DE PÁGINAS:	29
ÁREAS TEMÁTICAS:	Proteccion de Datos Personales, Derecho Constitucional, Derecho laboral		
PALABRAS CLAVES/ KEYWORDS:	Datos biométricos, Consentimiento libre, Huella digital, Protección de datos personales, Mecanismos de Control Asistencia, Datos sensibles.		
RESUMEN/ABSTRACT:	En el Ecuador la protección de datos personales ha sido un tema relevante el cual se vino a desarrollar con normativa en mayo del 2021, la promulgación de la Ley Orgánica de Protección de Datos Personales, esto generó en el Ecuador que los empleadores hagan uso de mecanismo de control de asistencias con el uso de los datos biométricos, que en este caso sería la huella digital. Este trabajo busca analizar el consentimiento de los trabajadores al momento del uso de la huella digital como método de asistencia, además si el consentimiento de los trabajadores podría recaer en una vulneración cuando se trate de otorgar sus datos biométricos como es el caso de la huella digital o si responde a una imposición implícita por parte del empleador y si esta es libre, específico e informado. Mediante un enfoque jurídico y normativo, aplicable en los ámbitos nacionales como internacionales. El estudio concluye con los vacíos normativos y prácticas empresariales que comprometen a los trabajadores, sugiriendo la necesidad de una regulación más precisa y que cuide los derechos de los trabajadores.		
ADJUNTO PDF:	☒ SI	☐ NO	
CONTACTO CON AUTOR/ES:	Teléfono: +593-998377277 - +593-986133007	E-mail: marialchevasco@gmail.com - xaviplazam@gmail.com	
CONTACTO CON LA INSTITUCIÓN (COORDINADOR 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):			