Facultad de Derecho

Tema:

Uso de datos biométricos (biometría) como método para aceptar las políticas de uso de datos personales.

Trabajo de Titulación para la obtención del Título de Abogado

Presentada por:

Ángel Ernesto Aguirre Mejía

Tutor:

Dr. Alberto Brown

Quito, junio de 2023

RESUMEN

Las personas a diario usan plataformas digitales que a su vez genera información, en su mayoría de carácter personal; sin embargo, para que terceros hagan uso de dicha informa personal es necesario el consentimiento del titular. Las plataformas digitales para obtener el consentimiento del titular establecen pequeños textos denominados políticas de privacidad; que, al ser aceptados permite que terceros puedan hacer tratamiento de sus datos personales. Los titulares de los datos, por falta de conocimiento, descuido o cualquier otro factor, aceptan las políticas de privacidad de forma automática y no razonada, afectando la formación del consentimiento y consigo el eje principal para la protección de datos personales. La ley Protección de datos personales de la legislación ecuatoriana (con sus limitaciones, si se la compara con otras legislaciones de la región), establece que la persona que recolecte este tipo de datos personales está en la obligación de establecer mecanismos de control y seguridad que resguarden a los datos personales de la recolección descontrolada. En el presente trabajo se sugiere y expone la utilización de la biometría por su creciente uso en el control de acceso, como un mecanismo de seguridad accesible y fácil de usar, mismo que encaja con nuestras leyes vigentes.

Palabras clave: Datos personales, consentimiento, políticas de privacidad, seguridad de la información, biometría.

DECLARACIÓN DE ACEPTACIÓN DE NORMA ÉTICA Y DERECHOS

El presente documento se ciñe a las normas éticas y reglamentarias de la Universidad Hemisferios. Así, declaro que lo contenido en este ha sido redactado con entera sujeción al respeto de los derechos de autor, citando adecuadamente las fuentes. Por tal motivo, autorizo a la Biblioteca a que haga pública su disponibilidad para lectura dentro de la institución, a la vez que autorizo el uso comercial de mi obra a la Universidad Hemisferios, siempre y cuando se me reconozca el cuarenta por ciento (40%) de los beneficios económicos resultantes de esta explotación.

Además, me comprometo a hacer constar, por todos los medios de publicación, difusión y distribución, que mi obra fue producida en el ámbito académico de la Universidad Hemisferios.

De comprobarse que no cumplí con las estipulaciones éticas, incurriendo en caso de plagio, me someto a las determinaciones que la propia Universidad plantee.

Nombre: Ángel Ernesto Aguirre Mejía

C.I. 1751066216

DEDICATORIA

Dedico este trabajo en primer lugar a mis abuelitos Mamá Clemencita y Papá Gonzalito que desde el cielo me iluminan para seguir adelante con mis proyectos.

A mi mami, por su inmenso amor, por su apoyo incondicional y por darme la fuerza para nunca rendirme. Por ser una mujer valiente, que siempre ha luchado por sus hijos para que podamos seguir adelante y ser hombres exitosos.

A mi papi, por sus valores y por siempre luchar por nuestra familia, que nunca nos falte nada. Por el sacrificio que siempre hace por sus hijos para que se conviertan en profesionales exitosos.

A mi hermano, por su apoyo incondicional en las buenas y en las malas.

A mi tío Arturo, por siempre apoyarme en conseguir mis metas.

Agradezco al Dr. Brown por acompañarme y guiarme en esta labor.

INDICE

USO DE DATOS BIOMÉTRICOS (BIOMETRÍA) COMO MÉTODO PARA ACEPTAR LAS POLÍTICAS DE USO DE DATOS PERSONALES.

Ángel Ernesto Aguirre Mejía

angelyag1313@gmail.com

RESUMEN

Las personas a diario usan plataformas digitales que a su vez genera información, en su mayoría de carácter personal; sin embargo, para que terceros hagan uso de dicha informa personal es necesario el consentimiento del titular. Las plataformas digitales para obtener el consentimiento del titular establecen pequeños textos denominados políticas de privacidad; que, al ser aceptados permite que terceros puedan hacer tratamiento de sus datos personales. Los titulares de los datos, por falta de conocimiento, descuido o cualquier otro factor, aceptan las políticas de privacidad de forma automática y no razonada, afectando la formación del consentimiento y consigo el eje principal para la protección de datos personales. La ley Protección de datos personales de la legislación ecuatoriana (con sus limitaciones, si se la compara con otras legislaciones de la región), establece que la persona que recolecte este tipo de datos personales está en la obligación de establecer mecanismos de control y seguridad que resguarden a los datos personales de la recolección descontrolada. En el presente trabajo se sugiere y expone la utilización de la biometría por su creciente uso en el control de acceso, como un mecanismo de seguridad accesible y fácil de usar, mismo que encaja con nuestras leyes vigentes.

Palabras clave: Datos personales, consentimiento, políticas de privacidad, seguridad de la información, biometría.

ABSTRACT

People daily use digital platforms that generate information, mostly of personal information; although, if other people want to use that information, a permission from the owner is required. In other to obtain that permission, those digital platforms establish small texts known as Privacy Policies; that if it is accepted, it allows that other can modify their personal data. The owners of the account, maybe lacking knowledge or any other factor, accept those Privacy Policies without thinking or in an automatic way, affecting the formation of consent and with it the main axis for the protection of personal data. The Ecuadorian Personal Data Protection Law (with its limitation, if compared to other laws in the region), establishes that the person who collects this type of personal data is obliged to establish control and security mechanisms that protect personal data from uncontrolled collection. In this work, the use of biometrics is suggested and expose due to its increasing use in access control, as an accessible and easy-to-use security mechanism, which fits with our current laws.

Key words: personal data, consent, Privacy Policies, Information security, biometrics

INTRODUCCIÓN

> "Los juristas debemos realizar un esfuerzo para superar la tendencia congénita a escanciar el vino nuevo de las cuestiones que emergen del cambio social tecnológico en los odres viejos conceptuales metódicos de la dogmática jurídica tradicional." – Pérez Luño

Con la pandemia del virus SARS-CoV-2 se ha acelerado el proceso de transformación digital y consigo la dependencia de las personas al uso de las TIC (Tecnologías de la información y comunicación). Las personas pudieron y tuvieron que continuar desarrollando sus actividades con ayuda de la tecnología, por ejemplo: desarrollar la actividad profesional por medio del teletrabajo, realizar compras por páginas web o adquirir una educación en modalidad no presencial. (Gómez-Córdoba, Arévalo-Leal, Bernal-Camargo, & Ríos, 2020) El uso de dichas tecnologías produce datos, en su mayoría de carácter personal; sin embargo, esto puede permitir el mal uso de dichos datos y la vulneración a la privacidad de las personas. (Bayés, Carmenati, & Apolo, 2017)

Cuando los usuarios entran a una página web o descargan alguna aplicación, se encuentran con un mensaje exigiendo al usuario la cesión de sus datos personales para poder usar dicha plataforma. El simple gesto de hacer un clic o marcar la palabra "aceptar" cede una incontable cantidad de datos personales. La política de privacidad explica el tratamiento que se dará a los datos personales y quienes harán uso de las mismas. Cuando los usuarios aceptan las políticas de privacidad, su información deja de ser privada y es compartida a terceros. Para que una persona o entidad responsable pueda tratar datos personales del titular, es necesaria la existencia del consentimiento; que se manifiesta con la aceptación de las políticas de privacidad. Las personas en la mayoría de casos acepta a ciegas, por desconocimiento o simplemente elude lo establecido en las políticas; aun cuando esto afecte o genere algún daño al titular de los datos personales recolectados. (Bayés, Carmenati, & Apolo, 2017)

El estudio "Conocimientos y comportamientos de los usuarios de la red social Facebook relacionados con la privacidad" de Durán-Segura M. et al. realizado en la Universidad de Sevilla y publicado en 2014; donde se examina tres variables relacionadas

con la privacidad de la información por Facebook. Para el desarrollo del presente trabajo se cita el factor relacionado al conocimiento real que tienen los encuestados sobre la política de privacidad de Facebook. La encuesta fue realizada a 190 jóvenes de entre 20 y 24 años de edad, 68 hombre y 122 mujeres, todos son usuarios de la plataforma Facebook. El 64% por ciento de los participantes afirmó nunca haber leído las políticas de privacidad, seguido del 18% que afirmó haber leído las políticas hace más de 6 meses. Con los datos antes mencionadas, la investigación concluyó que los usuarios aceptan las políticas sin leerlas. (Segura & Peligro, 2014)

Las nuevas normativas de protección de datos personales como la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) de la legislación española promulgada en 2018; basada a su vez en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea del 2016, han actualizado y regulado su normativa con las problemáticas actuales. Las normativas antes mencionadas sugieren la implementación de mecanismos de seguridad para los usuarios y mayores obligaciones para las personas y entidades responsables de la recolección de datos personales. La Ley Orgánica de Protección de Datos Personales ecuatoriana determina que el responsable del tratamiento está en la obligación de implementar medidas técnicas y organizativas apropiadas que garantice la seguridad e integridad de la información. (Asamblea Nacional Del Ecuador, 2021)

El ordenamiento jurídico nacional en la Ley Orgánica de Protección de Datos (LOPDP) de 2021 exigen la existencia del consentimiento; por dicha razón se establece la obligación por parte del responsable de invertir en sistemas de seguridad que controle el acceso. El principal problema en el proceso de recolección, es la identificación del usuario, existiendo mayor riesgo de suplantación de identidad a la hora se aceptar el consentimiento. (López, 2001) Los métodos alternos pueden aumentar la versatilidad del proceso de recolección de datos, por esta razón se propone la implementación de métodos de seguridad basados en la autenticación, como la biometría.

CAPÍTULO I

DATOS PERSONALES

En el Ecuador, se reconoce la protección de datos personales en el artículo 66 numeral 19 de la Constitución, que establece lo siguiente: "La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o por el mandato de la ley"[1]. Es indispensable que exista el consentimiento por parte del titular de la información para que se puedan utilizar sus datos personales por terceros. Otro tecnicismo al que se debemos hacer referencia y que la Constitución establece en el artículo antes mencionado es la protección del dato como información: "El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter"[1]. (Asamblea Nacional Constituyente, 2008)

Primero debemos definir qué se entiende por dato; según Quesada, J. un dato es: "Un dato puede ser entendido como una pieza de información carente de una estructura que le aporte significado"[2]. Es decir que un "dato" por sí mismo no tiene mayor relevancia, mientras que, cuando se constituye en un "conjunto de datos" estructurados conforma información de relevancia. Se plantea que la información es el conjunto de datos que producen una conclusión. En otras palabras, es el resultado de interpretar datos de manera que den un sentido o representen un significado. Incluso los datos considerados como irrelevantes, pueden conformar características que configuran el perfil del titular, en este punto ya estaríamos hablando de información personal. Se puede decir que la normativa vigente nacional (LOPDP) tutela toda posible vulneración de los datos de carácter personal. Se puede indicar, que el "dato" sería susceptible de protección por la posibilidad de llegar a tener un significado y consigo configurar la privacidad y seguridad de un ser humano. (Quesada, 2011)

El objetivo de la protección de datos de carácter personal es la autodeterminación informativa, que según Hassemer W. se entiende como: "aquella necesidad de que los

[1] Asamblea Nacional Constituyente. (2008). *Constitución De La República Del Ecuador.* (Registro Oficial No. 449). Ecuador.
[2] Quesada, J. C. (septiembre de 2011). *La Diferenciación Entre Dato, Información y Conocimiento: Una Precisión Más Necesaria Que Nunca.* Obtenido de Academia: https://www.academia.edu/2767609/Dato_informacion_y_comocimiento

ciudadanos controlen la información que les concierne, ya no como un mero derecho de defensa frente a las intromisiones de otros, sino ahora, y frente a los riesgos tecnológicos, como un derecho activo de control sobre el flujo de informaciones que circulan sobre nosotros"[3]. Es decir, es la potestad que tiene el individuo para decidir por sí mismo; es así que el fin de la protección de datos personales, es amparar a los titulares de la información personal para que sus datos no caigan en manos de terceros sin su consentimiento. El consentimiento es un factor indispensable para que el titular determine que otras personas usen sus datos de carácter personal. (Villalba-Fiallos, 2017)

Por otro lado, la protección de datos personales no está protegiendo el dato como tal, sino lo que se procura proteger es al titular de los datos. Es decir, no es la informática la que se procura proteger, sino la utilización que se puede hacer de la misma la que podría afectar a la libertad individual, como se contempla en la Constitución ecuatoriana de 2008 y también afecta a los intereses del titular. Entonces la información personal que es la unión del titular y del dato, es el motivo de protección, frente al manejo indebido, producto de la falta de aprobación del titular. (H. Cámara De Diputados, 2010)

La normativa de protección a los datos personales garantiza al titular el respeto de su propia identidad, por lo que busca es impedir la instrumentalización del ser humano.

Los datos personales tienen un valor innegable, el titular debe ser consciente de su gran importancia y comenzar a actuar en consecuencia del tratamiento de su propia información personal. (H. Cámara De Diputados, 2010) El mismo titular es el responsable sobre el uso que le puede dar a sus datos personales. Debe ser sensato sobre qué tipo de cuidado y limites desea para el trato de su propia información personal.

En definitiva, los datos tienen carácter personal cuando se crean perfiles y permiten inferir las características únicas del titular, permitiendo identificar a uno con otro. Tomando en cuenta todo lo mencionado anteriormente, los datos personales son definidos según Robles-Hernández J. como: "Toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de ser recogida"[4]. A su vez, el Parlamento Europeo y el Consejo de la Unión Europea lo definen como:

[3] Hassemer, W., & Sánchez, A. C. (1997). *El Derecho a La Autodeterminación Informativa Y Los Retos Del Procesamiento Automatizado De Datos Personales*. Buenos Aires: Del Puerto

[4] Robles-Hernández, J. G. (2004). *Derecho De La Información Y Comunicación Pública*. México: Edit. Universidad De Occidente.

> "Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"[5].

Cabe mencionar que los datos que permiten la identificación de las personas dejan de ser sensibles cuando su información es destinada a ser pública. Cuando un tercero maneja los datos del titular sin su consentimiento, a tal punto que atente contra su intimidad y su privacidad, le quita al titular la plena libertad para disponer sobre su manejo, yendo en contra de lo que salvaguarda la protección de datos personales. (Saltos & Andrade, 2019) Así lo establece el Tribunal Constitucional de España, determinado que la protección de datos personales garantiza a las personas un poder de control sobre sus datos personales. Por su parte en el Ecuador se reconoce la protección de datos personales, que mediante mandato constitucional determina que el titular a través de la formación de su consentimiento puede ceder a terceros para que hagan tratamiento de sus datos personales. (Sentencia 292/2000, 2001)

Por otra parte, todos tenemos derecho de saber quién maneja nuestros datos y cómo los maneja, es decir, poseer un control para proteger nuestra intimidad y privacidad que es la base de la protección de datos personales según el artículo 12 de la Declaración universal de Derechos Humanos de 1948.

Es importante entender el derecho a la intimidad y a la privacidad, de los cuáles brota otro concepto complementario que es la vida privada, que son conceptos claves para determinar cuándo se estaría atentando con la protección de datos personales. Es importante resaltar que en la Constitución ecuatoriana en el artículo 66 numeral 20 se reconoce el derecho a la intimidad. Por su parte, en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de la legislación ecuatoriana, mencionaba en el artículo 9 (artículo derogado en el 2021), en el que se reconocía el derecho de intimidad y privacidad, estableciendo: "La recopilación y uso de datos personales responderá a los

[5] Parlamento Europeo Y Consejo De La Unión Europea. (2016). *Reglamento (UE) 2016/679 Del Parlamento Europeo - Reglamento General De Protección De Datos*. Diario Oficial De La Unión Europea.

derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad"[6].

En la actualidad, con el avance de la tecnología es una prioridad la conservación de la intimidad y la reserva de los datos de las personas, siendo más accesible al conocimiento ajeno.

La intimidad y privacidad son conceptos que van ligados a la protección de datos personales, que se derivan del reconocimiento a la libertad, como lo determina la Constitución ecuatoriana "capítulo VI" derechos de libertad y continúan con el reconocimiento de la protección de datos y el derecho a la intimidad; por lo tanto, estos dos conceptos se definirán a continuación:

Intimidad: se entiende como una barrera de protección que salvaguarda lo más cercano del titular, algo interno o reservado del titular o que proyecta su entorno. La intimidad se establece con la vivencia particular de un mundo interno, cuyos elementos pueden ser los siguientes: sentimientos, autovaloraciones, pensamientos o procederes y también con la vivencia del exterior: personal, grupal o familiar. (Fajardo, 2006) En definitiva, la intimidad es la defensa ante cualquier incursión que se pueda dar en el ámbito interno exclusivo que incumbe únicamente al titular, quien puede resguardar aquel conjunto de experiencias, sentimientos y conductas personalísimas.

Privacidad: Haciendo una recapitulación, dijimos que la intimidad pertenece a la esfera más reservada del individuo, en el ámbito de lo personal. Por su parte, la privacidad es la libertad que tienen las personas ante el contacto con la sociedad y ante la contemplación de los demás. Es decir, se comprende como la facultad que tienen los individuos para disponer voluntariamente de un retiro de la vida en sociedad. (Fajardo, 2006) La privacidad tiene tres características esenciales: "El secreto, anonimato y la soledad"[7]. Según Bidart-Campos la intimidad y la privacidad se define como: "La intimidad es la esfera personal que está exenta del conocimiento generalizado de tercero...

[6] Congreso Nacional Del Ecuador. (17 de abril de 2002). *Ley De Comercio Electrónico, Firmas Y Mensajes De Datos*. Ecuador: Registro Oficial Suplemento 557.
[7] Sanz-Salguero, F. J. (2018). *Delimitación De Las Esferas De La Vida Privada, Privacidad E Intimidad, Frente Al Ámbito De Lo Público.* Transparencia & Sociedad (6), 127-149.

y la privacidad es la posibilidad irrestricta de realizar acciones privadas (que no dañen a otros) que se cumplan a la vista de los demás y que sean conocidas por estos"[8].

Cuando se habla de lo privado, se refiere a lo restringido, conocido por unos pocos y protegido frente a terceros, que al igual de que la intimidad protege la inviolabilidad de la personalidad del individuo. En efecto, la privacidad es definida como "el derecho que tienen los individuos a determinar la manera, espacio y tiempo en que la información que les concierne como personas, es decir, se habla de los aspectos de la persona que puede ser comunicada a otra"[9]. Como lo establece la definición citada, los aspectos de la persona de manera individual no adquieren un especial significado, solo al ser ponderados de manera conjunta relevan un perfil de la personalidad de la persona, y entonces debe ser defendido frente los riegos del uso de la información. En relación con la protección de datos personales, que es el tema a tratar, el fin no es proteger únicamente a la intimidad, sino la integridad física y mental de las personas evitando toda intromisión no consentida en la vida privada. Es decir, la intimidad y privacidad tienen diferente significado, pero su fin es el mismo, la protección de la integridad del ser humano. (Sanz-Salguero, 2018)

Vida privada: El derecho a la vida privada es reconocido como un derecho humano, pero no existe una definición que describa con claridad este término. Así lo ha explicado la Corte Interamericana de Derechos Humanos: "El concepto de vida privada es un término amplio no susceptible de definiciones exhaustivas"[10]. En el mismo fallo estableció una aproximación de lo que puede ser: "La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectarla hacia los demás"[10.]

Es decir, es ese derecho que tienen las personas para mantener fuera del conocimiento de terceros, las virtudes de la vida corporal y espiritual que le produce al individuo, aun cuando no afecten a la personalidad del individuo, es decir, cuando le resulte íntimo. En efecto, la vida privada se entiende como el derecho que tiene una persona de ser libre y llevar su vida como lo desee, siempre tomando en consideración los límites para la perfecta armonización entre los intereses del titular y el resto de la

[8] Villalba-Fiallos, A. (2017). *Reflexiones Jurídicas Sobre La Protección De Datos Y El Derecho A La Intimidad En La Autodeterminación Informativa.* FORO - Revista De Derecho (27), 23-42.
[9] Robles-Hernández, J. G. (2004). *Derecho De La Información Y Comunicación Pública.* México: Edit. Universidad De Occidente.
[10] Caso Atala Riffo Y Niñas Vs. Chile (Corte Interamericana De Derechos Humanos 24 de febrero de 2012).

sociedad. (Fajardo, 2006) Por esta razón Fajardo I. estable que: "Las personas tienen una esfera mínima de libertad personal que no puede ser invadida por nadie"[11].

En definitiva, la protección de datos personales es un derecho y un mecanismo de protección que ampara varias dimensiones del derecho a la intimidad, la privacidad y a la vida privada. (Fajardo, 2006) Una vez desarrollado estos tres conceptos nos basaremos en el lugar donde más se ven afectados.

En la actualidad vivimos en el auge del desarrollo tecnológico y el fácil acceso al internet. De acuerdo con el estudio "Política de privacidad en la Internet: noción y tecnología" de Gonzales H. del año 2006, se podría indicar que la mayoría de los usuarios no tienen el conocimiento necesario sobre el manejo que le darán a sus datos entregados mediante links, encuestas y redes sociales. (González, 2006)

Por lo anotado, las personas desconocen la totalidad del riesgo y la necesidad de proteger los datos personales, por lo que a diario miles de personas que navegan por la web ofrecen su información personal de manera involuntaria o confían su información sin saber que función le dará a los datos proporcionados. (Qués, 2014) Convirtiendo al avance de la tecnología el medio más fácil de conseguir datos; arrastrando a posibles vulneraciones, siendo la protección de datos el instrumento para proteger los derechos fundamentales que abarca este tema y brindar mayor seguridad jurídica a los titulares. (Roldán-Carrillo, 2021)

1.1. Política de privacidad

La política de privacidad está establecida en la Ley Orgánica de Protección de Datos Personales (LOPDP) de la legislación ecuatoriana, en el artículo 47 numeral 4 disponiendo que el responsable del tratamiento de datos personales está en la obligación de: "Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular"[12]. La legislación ecuatoriana no define expresamente lo que son las políticas o el aviso de privacidad, aunque es implementado a nivel internacional no se encuentra establecido específicamente en una normativa nacional. En otras legislaciones como Ley de Protección de Datos Personales de la

[11] Fajardo, I. A. (2006). *Aproximación Conceptual Al Derecho A La Intimidad*. Derecho Y Realidad (7), 191-202.
[12] Asamblea Nacional Del Ecuador. (2011). *Ley Orgánica De Protección De Datos Personales.* (Registro Oficial No. 459), Quinto Suplemento Del Registro Oficial. Ecuador.

legislación colombiana los conceptos de política de privacidad y aviso de privacidad se basan con los principios que se encuentran en el artículo 10 de la LOPDP de la legislación ecuatoriana, para poder conceptualizarlos. (Asamblea Nacional Del Ecuador, 2021)

La política de privacidad que se está tratando en el presente estudio nace del "principio de responsabilidad proactiva y demostrada" que establece:

> "El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento"[13].

El "principio de responsabilidad proactiva y demostrada", establece la obligación del responsable del tratamiento que recoge y hace tratamiento de datos personales, en asegurar el cumplimiento de los demás principios, establecer medidas para su aplicación y demostrar que se cumple con las obligaciones establecidas en la LOPDP. El principio de responsabilidad tiene muchas acepciones, pero en el ámbito de protección de datos personales este principio es conocido como principio de responsabilidad proactiva o accountability (en inglés). Dicho principio resalta la participación del responsable del tratamiento de datos y la adecuación de medidas internas dentro de cada organización que le permitan cumplir con lo establecidos en las leyes de protección de datos personales. La finalidad del principio antes mencionado es que el responsable del tratamiento de datos se comprometa a incrementar los estándares de protección de datos personales, garantizando a los usuarios un tratamiento adecuado de su información personal. (Huerta, 2022)

La herramienta o medida más utilizada por los responsables del tratamiento para cumplir con el principio de proactiva es la elaboración de políticas de privacidad que sean obligatorias de cumplir internamente en cada organización. Las políticas de privacidad se

[13] Asamblea Nacional Del Ecuador. (2021). *Ley Orgánica De Protección De Datos Personales.* (Registro Oficial No. 459), Quinto Suplemento Del Registro Oficial. Ecuador.

pueden entender según el National Institute of Standards and Technology (NIST) de EEUU, que lo define como: "Declaraciones, reglas o afirmaciones que especifican el comportamiento correcto o esperado de una entidad"[14]. Otra definición del mismo NIST, es la siguiente: "Reglas de seguridad específicas para un sistema o la política de seguridad de acceso remoto de una organización"[14]. La política de tratamiento de datos se entiende como un código de conducta, manual interno o mecanismo de certificación de políticas "reglas o afirmaciones" y procedimientos que indican el modo de actuar de los responsables de tratamiento de datos con el fin de cumplir con lo estipulado en la ley de protección de datos personales en un sistema de digital.

1.1.1. *Contenido de una política de privacidad*

El Reglamento General de Protección de Datos (RGPD) de la Unión Europa y el Decreto 1377 de 2013 en Colombia, ambas en el artículo 13 coinciden en varios puntos que debe contener una política de privacidad. En ambas normativas se establece que una política de privacidad puede constar por un medio escrito o electrónico y que debe ser lo más claro y comprensible posible para el titular. La política de privacidad de datos de manera general debe contener la siguiente información:

1. Datos del responsable o representante.
2. Información sobre la finalidad del tratamiento a que se destinan los datos personales con la debida base jurídica. Se establece cuales son los objetivos que busca la persona que recolecta y trata la información personal de los usuarios.
3. Licitud del procesamiento de los datos. El responsable está en el deber de informar al usuario de la licitud de la recolección y tratamiento.
4. Terceros destinatarios de los datos personales. En la política se informa al usuario si sus datos personales son enviados a terceras personas.
5. Plazo de conservación de los datos. Es el tiempo máximo que se almacenará y hará uso de los datos personales de los usuarios. En el caso de no existir un período de tiempo exacto, se establece un criterio que establece un plazo de conservación.
6. Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Los usuarios como titulares de sus derechos personales pueden acceder a ellos,

[14] Nieles, M., Dempsey, K., & Pillitteri, V. Y. (June 2017). *An Introduction To Information Security*. (Special Publication 800-12), Revision 1. U.S.A: National Institute Of Standards And Technology - U.S. Department Of Commerce.

rectificarlos, solicitar que se cancelen o se eliminen y oponerse a su uso. Los Derechos ARCO facultan a los titulares a tener control sobre sus datos personales, haciendo efectivo el poder disposición o mandato que tiene el titular y obliga al responsable a facilitar el ejercicio de dichos derechos.

Con los derechos ARCO el titular de los datos personales está en la facultad y responsabilidad de oponerse si un tercero maneja sus datos personales de forma distinta a la establecida en la LPDP.

A continuación, se describirán de manera breve los derechos ARCO:

- **Acceso:** Es la faculta del titular de acceder o ser informado por el responsable del tratamiento y uso que se les da a sus datos personales. (Roldán-Carrillo, 2021)
- **Rectificación y Actualización**: El titular tiene derecho a modificar, rectificar o actualizar los datos personales que sean inexacto o incompletos. (Roldán-Carrillo, 2021)
- **Cancelación o Eliminación:** Es el derecho que tiene el titular a que el responsable elimine o suprima del tratamiento sus datos personales. En el artículo 15 de la LOPDP de la legislación ecuatoriana establece las causales por las cuales se pueden eliminar los datos del tratamiento:

> " El tratamiento no cumpla con los principios establecidos en la ley, cuando el tratamiento no sea necesario para el cumplimiento de la finalidad, cuando los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados, cuando haya vencido el plazo de conservación de los datos personales, cuando el tratamiento afecte derechos fundamentales o libertades individuales, cuando revoque el consentimiento prestado o señale no haberlo otorgado y cuando exista una obligación legal"[15].

- **Oposición:** Es el derecho que tiene el titular para negar el tratamiento de sus datos o finalizar el uso de los mismos. La LOPDP de la

[15] Asamblea Nacional Del Ecuador. (2021). *Ley Orgánica De Protección De Datos Personales*. (Registro Oficial No. 459), Quinto Suplemento Del Registro Oficial. Ecuador.

legislación ecuatoriana en el artículo 16 las causales donde el titular puede aplicar el derecho de oposición.

El responsable puede implementar los demás derechos establecidos en la LOPDP. (Roldán-Carrillo, 2021)

En la legislación ecuatoriana no se habla expresamente de una política de privacidad, pero en el artículo 12 de la LOPDP establece el derecho a la información señalando que el titular de datos personales tiene derecho a ser informado por cualquier medio sobre las especificaciones establecidas en el mismo artículo. (Asamblea Nacional Del Ecuador, 2021)

1. 2. Aviso de privacidad

La legislación ecuatoriana no define lo que es el aviso de privacidad; sin embargo, el Decreto 1377 de 2013 de la legislación colombiana lo define como:

> "Un documento que puede ser trasmitido de forma verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales"[16].

El aviso de privacidad se relaciona con el principio de información y transparencia. El principio de información señala que el responsable del tratamiento debe informar al titular como primera etapa antes que se recopile información sobre la recolección y uso que se le dará a sus datos. Por la razón antes mencionada, el responsable debe informar al usuario sobre las políticas de privacidad por medio de un aviso de privacidad. (Novoa, 2020) Por su parte, el principio de transparencia que está definido en la LOPDP de la legislación ecuatoriana establece que: "El tratamiento de datos personales deberá ser transparente por lo que toda información o comunicación relativa a este

[16] *Decreto 1377 De 2013*. (27 de junio de 2013). Decreto. Bogotá, Colombia: El Diario Oficial 48834.

tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro"[17].

El Informe sobre políticas de privacidad en internet de la Agencia Española de Protección de Datos Personales (AEPD) del año 2018, establece que la información sobre el tratamiento de datos personales debe ser "concisa, transparente, de fácil acceso y con lenguaje claro y sencillo" recomendando que el documento donde se detalla dicho tratamiento debe ser de fácil comprensión y presentarse en un único texto dentro de un sistema digital. (Agencia Española De Protección De Datos Personales, 2018)

Como se mencionó anteriormente, en la legislación ecuatoriana no se encuentra establecida lo que es el aviso de privacidad, ni que lo debe contener; sin embargo, La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LPDPPSO) de la legislación mexicana establece que el aviso de privacidad tiene principalmente dos modalidades: El simplicado y el integral.

- **Simplicado:** Es un método que se utiliza para la recolección de datos del titular por a través de internet o alguna Tecnología de la Comunicación (TIC).
- **Integral:** Es un método que se utiliza para la recolección de datos del titular de manera presencial o física.

Para el entorno digital es común la utilización de hipertextos que se entiende como: "Enlazar piezas de información y utilizar esos enlaces para acceder a otras piezas de información relacionadas"[18]. El hipertexto es un elemento de información que puede constituir una simple idea, hasta un fragmento de un texto que facilita la presentación y funcionamiento del proceso del tratamiento de datos personales. Los hipertextos son usados por lo general como avisos de privacidad y van acompañados de enlaces o mejor conocidos como "links". Los links automáticamente dan acceso a otros documentos mediante un clic sobre dicha palabra o botón digital; es decir, que el aviso de privacidad debe contener dicho link que nos de acceso al documento en el que se establecen las políticas de privacidad. (Bayés, Carmenati, & Apolo, 2017) Esto va en concordancia con Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos (LCEFEYMD) de la legislación ecuatoriana, que en el artículo 3 establece: "Se reconoce validez jurídica

[17] Asamblea Nacional Del Ecuador. (2021). *Ley Orgánica De Protección De Datos Personales*. (Registro Oficial No. 459), Quinto Suplemento Del Registro Oficial. Ecuador.
[18] Cantos-Gómez, P., Martínez-Méndez, F. J., & Moya-Martínez, G. (1994). *Hipertexto Y Documentación.* Murcia, España: Universidad De Murcia.

a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes"[19].

1.2.1. *Contenido de un aviso de privacidad*

En el artículo 15 del Decreto 1377 de 2013 de la legislación colombiana establece requisitos mínimos que debe contener un aviso de privacidad:

1. Nombre del responsable del tratamiento.
2. El tratamiento al cual serán sometidos los datos y la finalidad del mismo.
3. Los derechos que protegen al titular.
4. Mecanismos dispuestos por el responsable para que el titular conozca la política de tratamiento de información.

Es imposible navegar por plataformas digitales como: Facebook, Outlook, LinkedIn, WhatsApp, entre otros muchos más; que son de uso habitual, sin que se recopile información. La recolección de datos se realiza con el consentimiento de los usuarios, en el momento que se acepta las Políticas de Privacidad al ingresar o crear una cuenta. (Zamudio-García, 2015)

Los sistemas digitales por lo general solicitan la información de los usuarios antes de otorgarles el permiso de ingreso, lo lamentable es que la mayoría de usuarios no leen las políticas de privacidad y no saben el uso que se le dará a dicha información. Por la razón antes mencionada, para que una persona este facultado en dar tratamiento de datos personales, es necesario que los usuarios acepten de manera inequívoca y concienzuda las políticas de privacidad. Todas las personas que haga tratamiento de datos de los usuarios están en la obligación de implementar una política de privacidad, para evitar sanciones y prevenir que se comenta algún ilícito con el uso de los datos de los usuarios. (De La Maza-Gazmuri & Momberg-Uribe, 2017)

[19] Congreso Nacional Del Ecuador. (17 de abril de 2002). *Ley De Comercio Electrónico, Firmas Y Mensajes De Datos*. Ecuador: Registro Oficial Suplemento 557.

CAPÍTULO II

CONSENTIMIENTO

El consentimiento desde una visión civilista se define como la manifestación y el acuerdo de voluntades entre dos o más personas, que presentan su conformidad de aceptar derechos y contraer obligaciones de dar, hacer o no hacer. (Llanos-Medina, 1944) Es decir, se perfecciona en el momento en que todas las personas naturales o jurídicas de la relación jurídica manifiestan su voluntad, direccionados a un mismo querer. Otro concepto que complementa al anterior, nos dice que el consentimiento es la aprobación de una persona que manifiesta su voluntad sin ningún vicio del consentimiento. (Arredondo-Galván, 2014)

Para entender la formación del consentimiento, debemos desglosar cada uno de los términos que la definen. Para que exista un acto jurídico o un negocio jurídico necesariamente debe existir voluntad, que según Stolfi, G. se define como: "La libertad que mantiene el individuo para relacionarse contractualmente con otros, pudiendo celebrar actos, determinar su contenido y efectos"[20].

De los elementos más importantes de la voluntad es su declaración, que está vinculada con la voluntad interna y el proceso de su manifestación. La voluntad es un fenómeno interno que se relaciona con la facultad de querer. De modo que no se puede comprobar porque pertenece a la voluntad de cada persona y es susceptible de cambios. (Amado, 1988)

Para integrar el consentimiento debe existir la integración de la oferta y la aceptación constituyendo así el negocio jurídico. Una de las partes propone una oferta y la otra manifiesta su aprobación, es decir, la aceptación se entendería como la declaración de voluntad. La aceptación constituye la consumación de un negocio jurídico produciendo consecuencias jurídicas, por lo que la voluntad de obligarse por parte del aceptante debe ser clara. (De Cuevillas, 2013)

La facultad que tienen los individuos para crear relaciones jurídicas mediante la manifestación de voluntad de cada miembro, debe ser necesariamente protegido contra la

[20] Stolfi, G. (2018). *Teoría Del Negocio Jurídico* (Primera ed.). Buenos Ares, Argentina: Ediciones Jurídicas Olejnik.

propia ignorancia de la persona y en contra de la influencia de terceros que pueden alterar la voluntad. (Stolfi, 2018)

Por esta razón, el acto jurídico no solo se formaliza con la aceptación de las partes para producir su voluntad, debe tener un grado de conciencia y voluntad. Con el fin, de que un acto no solo produzca efectos jurídicos, sino también que no tenga vicios que pueden generar su nulidad total o parcial del acto jurídico. (Llanos-Medina, 1944)

Si el proceso de formación de la voluntad es perturbado, al momento de exteriorizarse no se obtiene un verdadero acto de voluntad y se entendería que dicho acto sería declarado nulo. Por la desarmonía entre la voluntad y su manifestación, por lo que no tendría validez alguna. (Larrea-Holguín, 2008) Finalmente, el consentimiento se manifiesta de dos formas: de manera expresa o tácita.

La aceptación expresa es cuando el aceptante da a conocer la declaración de voluntad de manera verbal, escrita o cualquier otro medio que resulte inequívoco. En cambio, la aceptación tácita es cuando el aceptante lleva a cabo actos en los que se entiende la aceptación de su voluntad y denoten su conformidad con la oferta. (Arredondo-Galván, 2014)

El consentimiento expreso se divide en: verbal, escrito y signos inequívocos. En primer lugar, el consentimiento expreso verbal se entiende como aquello expresado con palabras, el consentimiento expreso escrito y finalmente el consentimiento expreso por signos inequívocos son aquellos que pueden interpretarse como una respuesta afirmativa de manera indudable. (Arredondo-Galván, 2014)

Una vez discutida la formación desde la noción del derecho civil, continuaremos desde un enfoque relacionado con la protección de datos personales que es nuestro tema principal a tratar. El artículo 9 (artículo derogado) de la Ley de Comercio Electrónico, Firma y Mensajes de datos de la legislación ecuatoriana, establecía que: "Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular"[21]. Comparando con otra legislación como la mexicana, establece que el consentimiento expreso se define: "El consentimiento será expreso cuando la voluntad

[21] Congreso Nacional Del Ecuador. (17 de abril de 2002). *Ley De Comercio Electrónico, Firmas Y Mensajes De Datos*. Ecuador: Registro Oficial Suplemento 557.

del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos"[22].

El consentimiento es el eje principal para protección de datos como se establece en el artículo 8 de la Ley Orgánica de Protección de Datos Personales de la legislación ecuatoriana, estableciendo que se puede manejar y anunciar datos personales cuando se cuente con la declaración de voluntad. (Roldán-Carrillo, 2021) La ley establece que el consentimiento es la manifestación de la voluntad libre, específica, informada e inequívoca. (Asamblea Nacional Del Ecuador, 2021) El titular es quien debe aprobar el tratamiento de sus datos personales, por lo que debe contar la aprobación para que el consentimiento sea válido.

La primera característica habla de la "libre voluntad", es decir, que no debe tener ningún vicio del consentimiento como lo establece la LOPDP de la legislación ecuatoriana, como complemento; el Código Civil ecuatoriano establece en el artículo 1467 tres vicios del consentimiento: Error, fuerza y dolo. (Enríquez-Álvarez, 2017)

A continuación, se desarrollará cada vicio del consentimiento:

Error: El Código Civil ecuatoriano no define el error, pero se limita a establecer los requisitos relevantes para que el error se configure. El error se lo define como: "Como el conocimiento falso de un hecho", es decir, es una forma incorrecta de ver la realidad. (Carrascosa-López, Pozo-Arranz, & Rodríguez-De Castro, 1996)

El error según el artículo 1468 del Código Civil ecuatoriano establece que el "error sobre un punto de derecho no vicia el consentimiento." En cambio, el artículo 1469 del código antes mencionado establece que "el error de hecho vicia el consentimiento". El error de hecho, como establece la normativa es la causal para que el consentimiento sea viciando. El error de hecho hace referencia a una confusión que ocurrió en un acto. (Carrascosa-López, Pozo-Arranz, & Rodríguez-De Castro, 1996)

Fuerza: El artículo 1472 del Código Civil ecuatoriano establece: "La fuerza no vicia el consentimiento, sino cuando es capaz de producir una impresión fuerte en una persona de sano juicio"[23]. Se entiende como la presión física o psicológica que se produce

[22] Cámara De Diputados Del H. Congreso De La Unión. (15 de julio de 2010). *Ley Federal De Protección De Datos Personales En Posesión De Los Particulares.* México: Diario Oficial De La Federación.
[23] Congreso Nacional Del Ecuador. (24 de junio de 2005). *Código Civil*. Ecuador: Suplemento Del Registro Oficial No. 46.

sobre una persona para ejecutar algún acto jurídico. (Carrascosa-López, Pozo-Arranz, & Rodríguez-De Castro, 1996)

Dolo: Se identifica con la mala fe o la mala intención con la que puede actuar una persona con otra. El artículo 1474 del Código Civil ecuatoriano establece: "El dolo da lugar solamente a la acción de perjuicios contra la persona o personas que lo han fraguado o que se han aprovechado de él; contra las primeras por el valor total de los perjuicios, y contra las segundas, hasta el valor del provecho que han reportado del dolo"[24].

El primer elemento cumple con lo establecido en la Unión Europea, el cual es regido por El Grupo de Trabajo del Artículo 29 que establece que: "el interesado puede elegir una opción real y no hay ningún riesgo de engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no consienta"[25].

La segunda característica habla de la "voluntad especifica", que se manifiesta si el titular mantiene una referencia clara del fin concreto y especifico que se dará a sus datos personales. La obligación que recae sobre la persona que hace el tratamiento de los datos del titular especificando cual es el proceso de tratamiento y la intención por la cual se están tratando los datos. Por este motivo, el titular debe determinar qué datos y que fines estarán destinados. (Roldán-Carrillo, 2021)

La tercera característica habla de la "voluntad informada", el responsable debe de manera previa otorgar la información de manera detallada sobre el tratamiento que se dará a sus datos, contribuyendo al entendimiento del titular. (Roldán-Carrillo, 2021) La LOPDP de la legislación ecuatoriana, establece que la voluntad informada va en conjunto con el principio de transparencia que establece que toda información o comunicación al tratamiento debe ser accesible y de fácil entendimiento. (Asamblea Nacional Del Ecuador, 2021)

La cuarta característica habla de la "voluntad inequívoca", hace referencia a la falta de dudas que debe tener el titular sobre el tratamiento que ejecutara el responsable a sus datos. (Roldán-Carrillo, 2021)

[24] Carrascosa-López, V., Pozo-Arranz, A., & Rodríguez-De Castro, E. (1996). *El Consentimiento Y Sus Vicios En Los Contratos Perfeccionados A Través De Medios Electrónicos.* Informática y Derecho: Revista Iberoamericana De Derecho Informático(2-15), 1021-1032.

[25] Grupo De Trabajo Del Artículo 29. (13 de mayo de 2020). *Directrices 5/2020 Sobre El Consentimiento En El Sentido Del Reglamento (UE) 2016/679.* Unión Europea: European Data Protección Board (EDPB).

La Ley de Protección de Datos Personales establece cuatro características de inevitable ejecución para que se configure la validez de la manifestación de la voluntad del titular, para el manejo de los datos personales del titular. En el caso de que no se cumpla con las cuatro características, se establece un acto ilegítimo al dar un tratamiento distinto al que fue establecido y que en especial atente contra los derechos fundamentales de las personas. (Enríquez-Álvarez, 2017)

La ley vigente de Comercio Electrónico, Firma y Mensajes de Datos (LCEFEYMD) de la legislación ecuatoriana en el artículo 48 establece el consentimiento para aceptar mensajes de datos determinado que "Previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes"[26]. El artículo citado al igual como se habló desde la visión civilista debe existir una oferta y una aceptación que pueden expresarse por medio de un mensaje de datos. El usuario al aceptar las políticas de privacidad (Oferta) presentado por el responsable del tratamiento, está consintiendo el uso de sus datos personales. (Bayés, Carmenati, & Apolo, 2017)

Los mensajes de datos según la LCEFEYMD de la legislación ecuatoriana, se definen como:

> "Toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos"[26].

El responsable del tratamiento debe implementar mecanismo para obtener la autorización del titular, dicha autorización puede contar en un documento electrónicos o mensaje de datos, es decir, lo denominado políticas de privacidad. (Bayés, Carmenati, & Apolo, 2017) Es importante recalcar que cuando se habla de consentimiento por medios electrónicos el Reglamento de Protección de datos de la Unión Europea en el artículo 32

[26] Asamblea Nacional Del Ecuador. (2021). *Ley Orgánica De Protección De Datos Personales.* (Registro Oficial No. 459), Quinto Suplemento Del Registro Oficial. Ecuador.

determina que el consentimiento puede ser de manera escrita o por medios electrónicos "Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales"[27].

[27] Parlamento Europeo Y Consejo De La Unión Europea. (2016). *Reglamento (UE) 2016/679 Del Parlamento Europeo - Reglamento General De Protección De Datos.* Diario Oficial De La Unión Europea.

CAPÍTULO III

SEGURIDAD DE LA INFORMACIÓN

El internet se ha vuelto un medio tan transitado que ha sido imparable y difícil de controlar, siendo sencillo acceder a información de manera ilimitada, pero no solo es un beneficio, también se incrementa el riesgo de que se atente contra derecho a la intimidad y a la vida privada. (Miguel-Pérez, 2015)

Es una herramienta útil para realizar numerosas gestiones sin salir de casa, por ejemplo, la compra de un producto por medio de plataformas o aplicaciones móviles. Otro fenómeno que actualmente ocurre es el uso de las redes sociales que nos permite estar conectados con otros usuarios y compartir información personal, de manera desproporcionada, es así que se genera información y constantemente se suministra información que es muy deseable por empresas, ciberdelincuentes o cualquier otra persona que se beneficie de los datos personales ajenos. (Alvarado, 2016)

La seguridad de la información se define como: "Aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada"[28]. La información es un activo valioso que debe ser protegida y controlada para que no se haga mal uso de ellos. En sentido general, la seguridad protege los activos de cualquier tipo de ataque de la mejor manera posible. Otro concepto de lo que significa la seguridad de la información es: "Proteger la información y los sistemas de información de un acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizada"[28.] La seguridad de la información es un concepto amplio que no se limitada a proteger un solo nivel de un proceso de protección de los datos y su objetivo es disminuir los riesgos que surgen por la presencia de amenazas para los activos, es decir, estaría en riesgo la información que se procesa, almacena o controla el acceso. (Miguel-Pérez, 2015)

[28] Vega-Briceño, E. (2021). *Seguridad De La Información*. Alicante, España: Editorial Área De Innovación Y Desarrollo, S.L.

La seguridad de datos personales es un principio establecido en la Ley Orgánica de Protección de Datos Personales de la legislación ecuatoriana, en el artículo 10 que determina:

> "Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales, frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto"[29].

Este principio general da a entender que es una exigencia que se impone a las personas encargadas del tratamiento de datos personales. Es decir, obliga a implementar medidas que garanticen la seguridad de los datos personales, para evitar su alteración, tratamiento y acceso no autorizado en las operaciones de recolección de datos, con el fin de evitar cualquier tratamiento ilegal o que afecten al titular de los datos personales. (Gómez-Vieites, 2011)

Esto garantiza la confidencialidad, integridad y disponibilidad, configurando la triada de la seguridad de la información. Estos tres pilares son principios bases para garantizar la seguridad de datos, proporcionando protección y la del entorno de la persona que proporciona los datos. Si no se desarrollan estos principios, la información se vuelve un blanco fácil para la manipulación y recolección no autorizada de datos personales. (Soriano, 2017)

A continuación, se desarrollará el principio de confidencialidad que es clave para el desarrollo del presente trabajo. La confidencialidad se refiere a la capacidad de proteger los datos del titular de aquellas personas que no están autorizadas por el titular para el uso de sus datos y que puede ser implementada en cualquier etapa del proceso recolección de datos. Es decir, es la capacidad de restringir el acceso a todos los usuarios no autorizados. (Vega-Briceño, 2021)

[29] Asamblea Nacional Del Ecuador. (2021). *Ley Orgánica De Protección De Datos Personales.* (Registro Oficial No. 459), Quinto Suplemento Del Registro Oficial. Ecuador.

La protección de datos personales garantizar el derecho de los titulares a determinar "cuándo, cómo, a quién, para qué y qué" información de carácter personal puede ser cedida a terceros. (Ribagorda-Garnacho, 2008)

Como establece el Tribunal Constitucional español en la sentencia del año 2000: "El derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"[30]. Por tanto, la seguridad informática juega un papel importante en la protección de datos, pues se ocupa en la protección del dato y consecutivamente de la información que tiene carácter personal. (Ribagorda-Garnacho, 2008)

Se debe considerar que la medida de seguridad que desarrollara en el presente trabajo al igual del resto de medidas de seguridad existentes van a tener sus fallas. Citando al autor Gene Spafford, "el único sistema seguro es aquel que está apagado en el interior de un bloque de hormigón, protegido en una habitación sellada rodeada por guardias armados"[31]. Con esta frase el autor nos permite entender que cualquier medida de seguridad que se presume razonable puede ser evadida y vulnerada, pero lo que se pretende es tener un mayor control en acceso de datos para que terceras personas no puedan tratar los datos personales del titular sin su automatización.

3.1 Medidas de seguridad

Para lograr una efectiva protección de datos personales es necesario establecer medidas tecnológicas que garanticen la seguridad de quienes emiten los datos personales. Las medidas de seguridad se concentran principalmente en mecanismos, sistemas y metodologías de la mano con los avances tecnológicos que facilitan el cumplimiento de los principios básicos de la protección de datos personales.

En el año 2003, la Comisión Europea, en el informe sobre la aplicación de la Directiva 95/46, sobre protección de datos, estable lo siguiente: "La aplicación de medidas tecnológicas adecuadas constituye un complemento fundamental de los medios

[30] *Sentencia 292/2000*, 1.463/2000 (Tribunal Constitucional De España 30 de noviembre de 2000).
[31] Vega-Briceño, E. (2021). *Seguridad De La Información*. Alicante, España: Editorial Área De Innovación Y Desarrollo,S.L.

jurídicos y debe constituir una parte de cualquier esfuerzo destinado a obtener un grado suficiente de protección de la intimidad"[32].

En el artículo 47, numeral 7 de la Ley Orgánica de Protección de Datos Personales de la legislación ecuatoriana establece lo siguiente: "Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas"[33]. Es una obligación de las personas responsables del tratamiento de datos personales, debiendo establecer medidas necesarias que dificulte la lesión contra la dignidad y la privacidad de las personas. (Comisión De Las Comunidades Europeas, 2007)

La Comunicación de la Comisión sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad, menciona que la protección que solo contempla medidas legales de protección resulta ser insuficiente debido a que los datos personales se difunden por todo el mundo por medio de redes de tecnologías de la información y la comunicación. El tratamiento de los datos personales del titular puede ocurrir en diferentes jurisdicciones, volviéndose sencillo atentar contra los derechos del titular de los datos personales, pudiendo quedar impune de las sanciones cometidas. (Vega-Briceño, 2021)

3.2 Identificación, autenticación y autorización

Existen muchas herramientas electrónicas que intentan suplantar el papel cuando se trata del consentimiento expresado de manera presencial. Los métodos alternativos pueden aumentar la versatilidad del procedimiento, además su uso presenta ventajas en relación con la seguridad y el control sobre el proceso. Estos nuevos métodos deben ser tomados en cuenta para garantizar que el proceso de información al usuario y posterior formación del consentimiento cumple con los requisitos establecidos en la norma.

El presente trabajo sugiere que la biometría sea implementada como una medida de seguridad de protección de datos personales y formación de consentimiento por medio del proceso de identificación, autentificación y autorización.

[32] Comisión De Las Comunidades Europeas. (2 de mayo de 2007). *Comunicación De La Comisión Al Parlamento Europeo Y Al Consejo Sobre El Fomento De La Protección De Datos Mediante Las Tecnologías De Protección Del Derecho a La Intimidad (PET).* Bruselas, Unión Europea.
[33] Asamblea Nacional Del Ecuador. (2021). *Ley Orgánica De Protección De Datos Personales.* (Registro Oficial No. 459), Quinto Suplemento Del Registro Oficial. Ecuador.

El Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos de carácter personal de la legislación española de 1999 define a la identificación y a la autenticación como:

Identificación: "Un procedimiento de reconocimiento de la identidad de un usuario". Es decir, mediante un procedimiento previo de verificación inequívoca de la identidad permite tener certeza de aquello.

Autenticación: "Un procedimiento de comprobación de la identidad de un usuario". Es decir, el usuario corrobora quien se supone que dice que es.

La autorización es un concepto que puede ser usado de diferentes formas, pero tiene un mismo fin. La autorización en sentido de seguridad de información se entiende como aquella que: "Protege los recursos importantes de un sistema, ya que limita el acceso solamente a los usuarios autorizados. Impide que los recursos se utilicen sin la autorización necesaria"[34]. El concepto antes mencionado va conjuntamente con el principio de seguridad y como se mencionó antes, la información personal sujeta a tratamiento deberá, establecer medidas técnicas para una mayor seguridad y protección de los datos personales.

La Constitución vigente de la República del Ecuador en el artículo 66 numeral 19 y la Ley de Protección de Datos Personales ecuatoriana hablan sobre el requerimiento necesario de la autorización para los responsables del tratamiento que recaban el consentimiento de los usuarios. La LOPDP ecuatoriana no establece algún concepto de lo que es la autorización direccionada en la protección de datos personales, pero la Ley de Comercio Electrónico, Firma Electrónicas y Mensajes de datos (LCEFEYMD) de la legislación ecuatoriana define a los datos personales autorizados como: "Aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular"[35].

Como se habló anteriormente, la persona que da tratamiento a datos personales está en la obligación de establecer mecanismos para obtener la autorización del titular,

[34] IBM. (20 de abril de 2021). *IBM MQ*. Obtenido de https://www.ibm.com/docs/es/ibm-mq/7.5?topic=ssfksj-7-5-0-com-ibm-mq-sec-doc-q009750--htm

[35] Congreso Nacional Del Ecuador. (17 de abril de 2002). *Ley De Comercio Electrónico, Firmas Y Mensajes De Datos*. Ecuador: Registro Oficial Suplemento 557.

convirtiéndose en una garantía el que se pueda verificar el otorgamiento de dicha autorización.

La identificación es la afirmación de lo que alguien o algo es, y la autenticación establece si la afirmación es cierta, finalmente con la identificación y la autenticación, se produce la autorización, que: "Una vez verificada la identidad del usuario se debe comprobar que dicho usuario tiene autorizado el acceso al servicio o al recurso que desea utilizar"[36]. Un ejemplo claro de identificación, es cuando se muestra la cédula de identidad, pasaporte o certificado de nacimiento, esto solo tiene el fin de verificar la identidad, no de autentificar.

Por su parte, la autenticación es "el conjunto de métodos que utilizamos para establecer un reclamo de identidad como verdadero"[37]. La autenticación tiene varios métodos que pueden ser usados, dividida en varias categorías que son: "Algo que sabes, algo que eres, algo que tienes"[37.] Para el desarrollo de este trabajo nos enfocaremos solo en la categoría de "Algo que eres" (La biometría). Es una categoría que se basa en los atributos físicos relativamente únicos de una persona. Los identificadores complejos como la huella dactilar, patrones de iris o características fáciles son más difíciles de falsificar o robar. A diferencia de estos, los atributos simples como la altura el peso, color de cabello y ojos no son lo suficientemente únicos como identificadores que puedan ser usados como medida de seguridad.

Los sistemas de verificación de identidad juegan un papel importante para evitar la suplantación y garantizar la seguridad de la información personal. La autenticación es esencial para obtener el consentimiento de manera virtual, limitándose a la confirmación de la identidad de una persona que acepta seguir con el proceso de verificación y acceso.

El concepto de la autorización es una parte esencial del trabajo. Una vez que se cumple con la recolección de datos, se requiere del consentimiento expreso con todos los requerimientos que establece el artículo 8 de la LOPDP de la legislación ecuatoriana. Es por eso que la mayoría de políticas de uso de datos personales solicitan una autorización previa para que sean tratados los datos personales de los usuarios para acceder a los

[36] Instituto Nacional De Tecnologías De La Comunicación (INTECO). (2012). *Guía Para Usuarios: Identidad Digital y Reputación Online.* España: Astrea.
[37] Registro Nacional De Identificación Y Estado Civil (RENIEC). (2015). *Identidad Digital. La Identificación Desde Los Registros Parroquiales Al DNI Electrónico.* Lima, Perú: PUNTO Y GRAFIA S.A.C.

servicios. Con la autorización se expresa de alguna manera la voluntad del usuario de aceptar los términos del manejo que se dará a sus datos personales. Con el proceso de la autorización consentida se asegura que el titular tiene conocimiento que su información será recogida y usada para fines determinados al margen del marco jurídico de la protección de datos personales.

Es esencial establecer mecanismos que restrinjan el acceso y permitan verificar que los usuarios que ingresan a un sitio web determinado son quienes dicen ser. El reconocimiento y validación de identidad de usuarios es indispensable para la autorización de acceso. El objetivo es que el acceso solo sea permitido para los usuarios que han sido autorizados. Para poder acceder al lugar restringido es necesario confirmar la identidad de las personas, tomando en cuenta la importancia de establecer mecanismos para validar el acceso. (Miguel-Pérez, 2015)

Una debida identificación acredita la identidad de las personas, vinculados con un determinado acto, declaración de voluntad o documento electrónico que gozan de validez y eficacia jurídica. La identificación es una herramienta que puede ser implementada por servicios, plataformas y sitios web que permite que una persona que se identifique y sea autenticada cumplida este proceso que confirma la identidad del usuario permite que el usuario tenga acceso al lugar restringido. La verificación de identidad garantiza la existencia de una persona detrás de una acción y "que es quien dice ser". (Martínez-Molano & Rincón-Cárdenas, 2021)

Las herramientas tecnológicas se crearon con el fin de brindad mayor facilidad y ayuda a los procedimientos que normalmente se hacían de manera presencial, pero no se puede negar que la identidad digital también tiene problemas en su desarrollo, siendo necesario tener claridad y verificación de quienes manejan los datos y la información que se proporciona. Pese a las posibles negativas que se pueden presentar al usar mecanismos de autentificación, la biometría, brinda protección a los usuarios y garantiza mayor seguridad a la información de carácter personal, permitiendo un mayor control de a quienes se proporciona información y que uso se dará. (Martínez-Molano & Rincón-Cárdenas, 2021)

CAPÍTULO VI

DATOS BIOMÉTRICOS

Desde tiempos inmemorables las personas han intentado tener mayor control en el acceso a lugares o información que consideran importante. Para poder acceder al lugar restringido, es necesaria la posesión de una llave o una clave. La información personal se ha convertido en un producto a la venta, generando la necesidad de desarrollar mejores sistemas de seguridad que controlen la divulgación de datos personales. (Machuca, Vinueza, Sampedro, & Santillán, 2022)

Las tecnologías biométricas producen beneficios en el aumento de los niveles de seguridad, además de ser accesible para la mayoría de usuarios que cuenten con un teléfono inteligente o cualquier otro medio tecnológico. En la actualidad, los métodos comúnmente usados como las contraseñas, números de PIN y tarjetas inteligentes pueden ser descifrados, copiados o robados. La tecnología biométrica aumenta la comodidad de los usuarios al no tener que recordar numerosas y complejas contraseñas o la perdida de las llaves acceso, permitiendo automatizar el procedimiento de reconocimiento biométrico. La tecnología biométrica tiene un sin número usos que pueden ser adaptados, incluso como medida de seguridad reforzado el acceso a los datos personales de los usuarios que se realiza mediante autenticación biométrica. (Observatorio De La Seguridad De La Información De INTECO, 2011)

La definición de datos biométricos se encuentra estipulado en el artículo 4 de la Ley Orgánica de Protección de Datos Personales ecuatoriana, que establece lo siguiente: "Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros"[38].

La Ley Orgánica de Protección de Datos Personales no se ha referido a detalle y con mayor profundidad al estudio de la biometría, siendo indispensable citar otras fuentes que definan el concepto de datos biométricos, como lo hace El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) de

[38] Asamblea Nacional Del Ecuador. (2021). *Ley Orgánica De Protección De Datos Personales.* (Registro Oficial No. 459), Quinto Suplemento Del Registro Oficial. Ecuador.

México en el 2018 que lo define como: "Propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles"[39].

La Ley de Protección de Datos Personales de la legislación ecuatoriana en el artículo 4 determina que existen características: físicas y de conducta. Es por esto que es importante describir a los rasgos biométricos, con sus diferentes tipos. Los aspectos físicos son, por ejemplo: la huella dactilar, la cara, el iris, o la geometría de la mano. Por su parte, los aspectos conductuales son, por ejemplo: la firma, la voz, la forma de caminar o pulsaciones del tecleo. La diferencia entre los aspectos biológicos y físicos, es que en los primeros se tiene que hacer dicha acción a diferencia de los aspectos físicos que se encuentra siempre presentes en la persona. (Ortega-García & Alonso-Fernández, 2008)

La Ley Orgánica de Protección de Datos Personales de la legislación ecuatoriana en el artículo 25 establece que los datos biométricos son datos sensibles que pertenecen a una categoría especial de los datos personales resaltando la importancia de resguardar y proporcionar una protección particular. Los datos biométricos deben ser tratados de forma muy sigilosa en el proceso de recopilación, almacenamiento y traspaso de los mismos.

Es fundamental que los estándares para el tratamiento de los datos biométricos sean mucho más estrictos, pero la normativa da una interpretación distinta. Los datos biométricos no deberían pertenecer a una categoría especial, porque las pocas regulaciones que tiene la biometría determinan que solo puede ser usados para identificar y autenticar de manera inequívoca a una persona. Por la razón antes mencionada es muy común que sean usados como medidas de seguridad para identificar y autentificar a una persona.

4.1. Biometría

La biometría no se conceptualiza en la normativa ecuatoriana, sin embargo, El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) de México en el 2018 establece: "Método de reconocimiento de personas basado en sus datos biométricos"[39]. El objetivo de usar características biométricas es obtener un conjunto de características físicas o conductuales que identifique o verifiquen la identidad de una persona. Para Yue Liu la biometría es lo

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

siguiente: “Mecanismos de medición de comportamiento o de las características físicas de las personas con miras a determinar o autenticar su identidad"[40].

Cualquier característica física o de comportamiento puede usarse como característica biometría, mientras cumpla con las siguientes particularidades:

- **Universalidad:** Todos los usuarios deben poseer esa característica.
- **Singularidad:** Las personas deben ser suficientemente diferentes adquiriendo una característica distintiva.
- **Permanencia:** El rasgo debe perdurar invariable en el tiempo.
- **Evaluabilidad:** El rasgo se mide cuantitativamente. Es decir, que son medibles o calculables.

Los parámetros que se extrae crean un patrón único de cada individuo para su posterior comparación.

Con el acelerado crecimiento de la tecnología biométrica, es muy común que esta se encuentre incorporada en los equipos portátiles o dispositivos móviles, siendo muy sencillo que las personas hagan uso de la misma. La biometría a diferencia de una llave, tarjeta de acceso o cualquier mecanismo de seguridad tradicional, usa aspectos propios de la persona que no pueden ser separados. La persona se vuelve la llave para tener acceso, convirtiéndose en el principal mecanismo de seguridad.

En el Ecuador, cada vez es más frecuente el uso de la biometría tanto en el sector público como privado. Un ejemplo en el Ecuador, donde se puede observar la aplicación de la biometría, es en la resolución Nro. 003-NG-DINARP-2022 de la Dirección Nacional de Registros Públicos que en el artículo 16, la validación a través de reconocimiento facial que establece “Se validará la identidad del usuario a través del software automatizado de identificación biométrica, capaz de identificar a una persona o de comprobar su identidad mediante la comparación…”[41]. Otro ejemplo en el Ecuador es el Acuerdo Ministerial 193 del Ministerio de Finanzas de 2012, que establece el uso obligatorio del sistema de autentificación biométrica, y finalmente en la Ley Orgánica de Gestión de la Identidad y

[40] Liu, Y. (2009). *The Principle Of Proportionality In Biometrics: Case Studies From Norway*. Computer Law & Security Review (25), 237–250.
[41] Dirección Nacional De Registros Públicos. (9 de agosto de 2022). *Resolución Nro. 003-NG-DINARP-2022*. Ecuador: Registro Oficial Nº 123.

Datos Civiles estable la captura de información biométrica con el fin de identificar a cada usuario.

4.2. Sistemas biométricos

La biometría se ha transformado en sinónimo de autentificación de los usuarios, usando las características únicas e irrepetibles por medio de los sistemas biométricos. Los sistemas biométricos según El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) de México en el 2008 establece: "Son las aplicaciones tecnológicas que permiten el reconocimiento automático de una persona a través de sus datos biométricos"[42]. Los sistemas biométricos están compuestos de dispositivos que recopilan características de la persona formado algoritmos y conforman las plantillas biométricas. Igualmente, el INAI establece que las plantillas biométricas son: "Representación alfanumérica de la información extraída de una o más muestras biométricas"[42.] Las plantillas se almacenan y se compara con los datos en la posterior actividad de verificación.

Los sistemas biométricos reconocen patrones que capturan datos biométricos de una persona, extrayendo un conjunto de particularidades que luego son comparados con otros patrones de datos. El sensor es el encargado de capturar el rasgo biométrico y un equipo biométrico es el encargado de medir, codificar, comparar, trasmitir y reconocer características personales. (Sánchez-Cortés, 2019) Un sistema biométrico determina dentro de la probabilidad estadística si la nueva plantilla coincide o no con las plantillas biométricas previamente recolectadas y almacenadas.

La identificación y autentificación biométrica es similar al enfoque antes mencionando en la seguridad de la información, sobre la cual se basan las medidas de seguridad. Según lo establecido en la Unión Europea, por en el Dictamen de 2012 por El Grupo de Trabajo del Artículo 29 que establece que la identificación biométrica ocurre cuando: "Un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos"[43]. Por otro lado, en el mismo dictamen se establece que la autenticación biométrica es: "La verificación de un individuo

[42] Instituto Nacional De Transparencia, Acceso a La Información Y Protección De Datos Personales. (2018). *Guía Para El Tratamiento De Datos Biométricos.* México: INAI.
[43] Grupo De Trabajo Del Artículo 29. (27 de abril de 2012). Dictamen 3/2012 Sobre La Evolución De Las Tecnologías Biométricas. Bruselas, Bélgica: Unión Europea.

por un sistema biométrico, es normalmente el proceso de comparación entre sus datos biométricos con una única plantilla biométrica almacenada en un dispositivo"[43.] El proceso completo de identificación y autentificación lo define como: "autentifican la identificación de la persona mediante la comparación del rasgo biométrico acabado de capturar con el rasgo biométrico que el sistema ha capturado antes en el proceso de inscripción al sistema"[43.]

En lo referente a las medidas de seguridad se debe establecer lo concerniente a la identificación y la autenticación, mismos que son adaptables en el proceso de reconocimiento biométrico, y que cumplen las siguientes fases:

Captura: Representación digital de los rasgos biométricos de los usuarios.

Registro: Se realiza a través de sensores que capturan muestras biométricas y se ingresan a la base de datos. Dependiendo del rasgo biométrico se necesita sensores adecuados.

Conversión: La muestra biométrica recopilada se convierte en una plantilla.

Almacenamiento: Se guarda las plantillas generadas en la fase de recolección o identificación.

Comparación: La nueva plantilla "obtenida de la captura en vivo" es comparada con las plantillas guardadas previamente por medio de cálculos algorítmicos.

Decisión: Se compara con las platillas registrada y se toma una decisión. (Instituto Nacional De Transparencia, Acceso a La Información Y Protección De Datos Personales, 2018)

La adecuación de los sistemas biometría reduce la falsa aceptación, negando el acceso a quien no está autorizado. El manejo de los datos personales es llevado de forma irresponsable por parte de los usuarios y con la implementación de los sistemas biométricos se trata de tener un mayor control de los datos entregados a terceros. Por el motivo antes mencionado, las apps, páginas web o cualquier servicio que se ofrezca en la red esta implementado los sistemas biométricos para cumplir con la normativa de protección de datos personales y tratar la información personal con los requerimientos de la ley.

4.3. Técnicas biométricas física y de comportamiento

El "Estudio Sobre Las Tecnologías Biométricas Aplicadas A La Seguridad" realizado por el Observatorio de la Seguridad de la Información del Instituto Nacional de Tecnologías de la Comunicación (INTECO) y publicado en 2011, desarrolla las principales técnicas biométricas físicas y de comportamiento. (Observatorio De La Seguridad De La Información De INTECO, 2011) A continuación, se desarrollará brevemente cada técnica:

4.3.1. *Físicas*

Las tecnologías biométricas físicas se distinguen por examinar factores derivados de los rasgos físicos de la persona; y son las siguientes:

Huella dactilar: Es la identificación de personas por medio del reconocimiento de por medio de las formas única e irrepetible de las huellas. Las huellas es un conjunto de "crestas" que son las líneas de la huella, "surcos" que son las hendiduras o abertura que existe en la huella y "minucias" que son los puntos donde terminan o continúan las crestas.

Reconocimiento facial: Es el reconocimiento de una persona a partir de una imagen o fotografía del rostro que se analiza diferentes ángulos, expresiones faciales, la forma de la nariz y la posición de la mandíbula. Cabe mencionar que esta técnica tiene falencias puesto que una persona puede medicar el aspecto de su cara.

Reconocimiento de iris: El iris es la parte que rodea a la pupila del ojo. Esta técnica analiza los patrones únicos, se analiza los "surcos" que es el grosor de la parte pigmentada del ojo y estrías del iris que se relacionada con la fisura y marcas que existen en dicha área.

Reconocimiento de retina: Los sistemas biométricos analizan la retina basando en el patrón de los vasos sanguíneos. Existen factores que podrían afectar a dicha técnica, por ejemplo, que el patrón se repita deje de ser único o que el patrón cambie con el tiempo.

Existen varias técnicas biométricas como la el reconocimiento de geometría de la mano, el reconocimiento de la geometría de las venas, por las muestras de ADN, por medio de algoritmos de la superficie de la piel, etc. Sin embargo, las técnicas biométricas física antes mencionada son las usadas y desarrolladas.

4.3.2. *Comportamiento*

Las tecnologías biométricas de comportamiento se distinguen por examinar factores derivados por las acciones realizadas por las personas.

Reconocimiento de firma: Esta técnica analiza la firma para confirmar la identidad de la persona titular del titular.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de la legislación ecuatoriana en el artículo en el artículo 13 establece que la firma electrónica sirve para identificar al titular de la firma e insinuar que el titular de la firma acepta la información contenida en un mensaje de datos. El artículo 16 de la ley antes mencionada establece que el mensaje de datos que sea firmado de forma electrónica supone la voluntad del titular de la firma. La firma como se establece en los artículos antes mencionados, es un dato biométrico, usado actualmente y reconocido en la legislación ecuatoriana para expresar el consentimiento de una persona. (Congreso Nacional Del Ecuador, 2002)

Reconocimiento de voz: Es una técnica de uso habitual que usan las personas para identificar a otras personas, por ejemplo: identificar una persona al oír una voz. Por medio de algoritmos se debe medir y evaluar si existe similitud, dando como resultado un resultado de posibles candidatos. Esta técnica tiene un margen de error por factores que pueden alterar la claridad de la voz como ruidos o la calidad de la muestra.

La tecnología biometría en el comportamiento está en desarrollo y no ha alcanzado los niveles de rendimiento necesarios para ser usados al igual que el resto de sistemas biométricos.

CONCLUSIONES

La protección de datos personales se reconoce y configura como un derecho establecido en la Constitución ecuatoriana en el artículo 66 numeral 19, que determina la protección de la información de carácter personal del titular. Los datos personales se relacionan principalmente con el derecho a la intimidad y privacidad de las personas, derechos que de igual manera tienen supremacía constitucional. El desarrollo de nuevas tecnologías de la información busca mejorar la vida de las personas, pero su uso también puede afectar los derechos vinculados con el derecho a la intimidad. Por las razones antes mencionadas el titular de los datos personales debe ser más cuidadoso en el uso de su información personal, saber a quién esta otorgado el manejo de sus datos personales y que fin se dará.

Para que los datos personales de los usuarios puedan ser tratados por terceros, es necesario su consentimiento, así lo estable en el artículo antes mencionado de la Constitución ecuatoriana. Los usuarios que navegan a través de plataformas digitales se encuentran con hipertextos que se titulan como "políticas de privacidad", por medio de estos mensajes se especifica que datos se recolectan y como serán tratados. Es común que los usuarios no lean las políticas de privacidad y simplemente con hacer un "clic" en el botón de "aceptar" se está consintiendo para que terceros puedan manejar los datos del titular a su conveniencia. La falta de control pone en riesgo la intimidad y privacidad; derechos fundamentales del titular, por la falta de dominio sobre la información personal que se transfiere a los responsables. El consentimiento como lo determina la LOPDP debe ser libre, especifico, informado e inequívoco requisitos que están siendo cumplidos para autorizar el tratamiento de los datos personales.

Con el desarrollo tecnológico, la recolección de datos por medio de internet se ha vuelto automatizado, lo que ha genera en la transmisión de datos personales sin la autorización del titular. Por dicha razón, la Ley de Protección de Datos Personales establece el principio de seguridad de información, que a través de medidas de seguridad permitan al titular tener mayor control sobre sus datos y evitar el acceso no autorizado. Las medidas de seguridad como lo establece ley, pueden ser variadas y son utilizadas como garantía para el titular de los datos personales.

La biometría actualmente tiene gran acogida en materia de privacidad y seguridad, cada vez es más común la implementación de sistemas biométricos para controlar el acceso no autorizado. El principal objetivo de la biometría es identificar y autentificar personas, mismo mecanismo usado para el proceso de control de acceso, para finalmente autorizar a las personas. La autorización se entiende como el consentimiento del titular para que sus datos personales sean tratados por terceros.

Finalmente, la biometría puede ser sugerida como un método para aceptar las políticas de privacidad y consigo expresar el consentimiento del titular para que sus datos personales se tratados por terceros. El dato biométrico actúa como una firma electrónica, que como lo determina la ley ecuatoriana supone la expresión del consentimiento del usuario. La legislación ecuatoriana puede acoger a la biometría como un método para otorgar el consentimiento por medio de la aceptación de las políticas de privacidad que se presenta en las plataformas digitales. La tecnología biométrica no es un método carente de riesgos de seguridad, pero a comparación de otras tecnologías es la más eficaz en el control de acceso, permitiendo a los usuarios conformar su consentimiento. Michael Palmer determina que: “los datos son el nuevo petróleo” del siglo XXI, por el uso que terceros pueden hacer con esa información, es por dicha razón que los datos personales deben ser protegidos de manera jurídica y técnica. Es por esto, que la biometría pretende ser un método técnico de protección de datos personales, que a su vez hace cumplir con la normativa ecuatoriana vigente de protección de dichos datos. Es decir, que la biometría permite restringir el acceso descontrolado y consecuentemente permite cumplir con la formación del consentimiento, eje principal para que los datos personales puedan ser transmitidos a terceros de forma legal.

BIBLIOGRAFÍA

- Agencia Española De Protección De Datos Personales. (septiembre de 2018). Informe Sobre Políticas De Privacidad En Internet - Adaptación Al RGPD. España.

- Alvarado, F. (2016). La Gestión De La Seguridad De La Información En El Régimen Peruano De Protección De Datos Personales. *Revista Foro Jurídico*(15), 26-41.

- Amado, J. D. (1988). Las Declaraciones De Voluntad Impropias En La Teoría Del Acto Jurídico. *THEMIS Revista De Derecho*(10), 75-88.

- Arredondo-Galván, F. X. (2014). *La Firma Electrónica Notarial Y La Copia Certificada Electrónica En El Distrito Federal. Colección Colegio De Notarios Del Distrito Federal.* México: Librería Porrúa.

- Asamblea Nacional Constituyente. (2008). Constitución De La República Del Ecuador. *(Registro Oficial No. 449)*. Ecuador.

- Asamblea Nacional Del Ecuador. (2021). Ley Orgánica De Protección De Datos Personales. *(Registro Oficial No. 459), Quinto Suplemento Del Registro Oficial*. Ecuador.

- Bayés, M., Carmenati, M., & Apolo, D. (2017). Privacidad En La Red: Una Aproximación Para El Análisis De Las Políticas De Google Y Facebook. *Comunicación, Igualdad Y Desarrollo, 7*(3), 231-250.

- Carrascosa-López, V., Pozo-Arranz, A., & Rodríguez-De Castro, E. (1996). El Consentimiento Y Sus Vicios En Los Contratos Perfeccionados A Través De Medios Electrónicos. *Informática y Derecho: Revista Iberoamericana De Derecho Informático*(2-15), 1021-1032.

- Comisión De Las Comunidades Europeas. (2 de mayo de 2007). Comunicación De La Comisión Al Parlamento Europeo Y Al Consejo Sobre El Fomento De La Protección De Datos Mediante Las Tecnologías De Protección Del Derecho a La Intimidad (PET). Bruselas, Unión Europea.

- Congreso Nacional Del Ecuador. (17 de abril de 2002). Ley De Comercio Electrónico, Firmas Y Mensajes De Datos. Ecuador: Registro Oficial Suplemento 557.

- De Cuevillas, I. (2013). El Concepto De Oferta Contractual En La Propuesta De Reglamento Opcional Sobre Una Normativa Común De Compraventa Europea (CESL) - Un Estudio a La Luz Del Derecho Civil Español. *Via Iuris*(15), 13-31.

- De La Maza-Gazmuri, I., & Momberg-Uribe, R. (2017). Términos Y Condiciones: Acerca Del Supuesto Carácter Contractual De Las Autorizaciones Para El Tratamiento De Datos Personales En Sitios Web. *Revista Chilena De Derecho Y Tecnología, 6*(2), 25-55.

- Enríquez-Álvarez, L. (2017). Paradigmas De La Protección De Datos Personales En Ecuador. Análisis Del Proyecto De Ley Orgánica De Protección a Los Derechos a La Intimidad Y Privacidad Sobre Los Datos Personales. *FORO-Revista De Derecho*(27), 43-61.

- Fajardo, I. A. (2006). Aproximación Conceptual Al Derecho A La Intimidad. *Derecho Y Realidad*(7), 191-202.

- Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Camargo, D., & Ríos, D. R. (2020). El Derecho A La Protección De Datos Personales, Tecnologías Digitales Y Pandemia Por COVID-19 En Colombia. *Revista De Bioética Y Derecho, 50*, 271-294.

- Gómez-Vieites, Á. (2011). *Enciclopedia De La Seguridad Informática* (Segunda ed.). España: RA-MA S.A.

- González, H. R. (agosto de 2006). Política De Privacidad En La Internet: Noción Y Tecnología. Neuquén, Argentina.

- H. Cámara De Diputados. (2010). *Protección De Datos Personales - Compendio De Lecturas Y Legislación* (Primera ed.). México: D.R Tiro Corto Editores.

- Huerta, J. (31 de agosto de 2022). *¿Aviso De Privacidad o Política De Privacidad?* Obtenido de https://es.linkedin.com/pulse/aviso-de-privacidad-o-pol%C3%ADtica-julio-huerta-

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

- Larrea-Holguín, J. (2008). *Manual Elemental De Derecho Civil Del Ecuador* (Corregida Y Actualizada ed., Vol. IV). Quito, Ecuador: Corporación De Estudios y Publicaciones (CEP).

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

- López, L. F. (2001). La Firma Electrónica En El Derecho Privado. *Revista Jurídica 5*, 41-68.

- Machuca, S. A., Vinueza, N. V., Sampedro, C. R., & Santillán, A. L. (2022). Habeas Data Y Protección De Datos Personales En La Gestión De Las Bases De Datos. *Universidad Y Sociedad. Revista Científica De La Universidad De Cienfuegos, 14*(2), 244-251.

- Martínez-Molano, V., & Rincón-Cárdenas, E. (2021). Problemas Y Desarrollo De La Identidad En El Mundo Digital. *Revista Chilena De Derecho Y Tecnología, 10*(2), 251-276.

- Miguel-Pérez, J. C. (2015). *Protección De Datos Y Seguridad De La Información* (Cuarta ed.). Madrid, España: Ra-Ma S.A.

- Novoa, E. (2020). El Derecho A La Protección De Datos De Personales En La Prestación De Servicios De Cloud Computing. Una Perspectiva Ecuatoriana. *Revista De Derecho*(22), 64-89.

- Observatorio De La Seguridad De La Información De INTECO. (2011). *Estudio Sobre Las Tecnologías Biométricas Aplicadas a La Seguridad.* España: Plan Avanza2.

- Ortega-García, J., & Alonso-Fernández, F. (2008). *Biometría y Seguridad* (Primera ed.). Madrid, España: Fundación Rogelio Segovia Para El Desarrollo De Las Telecomunicaciones.

- Qués, M. E. (2014). *Datos Personales Y Nuevas Tecnologías.* Buenos Aires, Argentina: Educ.Ar S.E.

- Quesada, J. C. (septiembre de 2011). *La Diferenciación Entre Dato, Información y Conocimiento: Una Precisión Más Necesaria Que Nunca.* Obtenido de Academia: https://www.academia.edu/2767609/Dato_informacion_y_comocimiento

- Ribagorda-Garnacho, A. (2008). La Protección De Datos Personales Y La Seguridad De La Información. *Revista Jurídica De Castilla Y León*(16), 373-400.

- Roldán-Carrillo, F. N. (2021). Los Ejes Centrales De La Protección De Datos: Consentimiento Y Finalidad. Críticas Y Propuestas Hacia Una Regulación De La Protección De Datos Personales En Ecuador. *USFQ Law Review, 8*(1), 175-202.

- Saltos, M. A., & 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, 6*(1), 233-254.

- Sánchez-Cortés, L. (febrero de 2019). Manual Para El Uso De Los Datos Biometricos En Los Servicios Financieros. México: INFOTEC Centro De Investigación E Innovación En Tecnologías De La Información Y Comunicación.

- Sanz-Salguero, F. J. (2018). Delimitación De Las Esferas De La Vida Privada, Privacidad E Intimidad, Frente Al Ámbito De Lo Público. *Transparencia & Sociedad*(6), 127-149.

- Segura, M. D., & Peligro, J. F. (2014). Conocimientos Y Comportamientos De Los Usuarios De La Red Social Facebook Relacionados Con La Privacidad. *Ambitos: Revista Internacional De Comunicación*(26), 231-240.

- Sentencia 292/2000 (Tribunal Constitucional De España 4 de enero de 2001).

- Soriano, M. (2017). *Seguridad En Redes Y Seguridad De La Información* . Praga, República Checa: České Vysoké Učení Technické V Praze - TechPedia.

- Stolfi, G. (2018). *Teoría Del Negocio Jurídico* (Primera ed.). Buenos Ares, Argentina: Ediciones Jurídicas Olejnik.

- Vega-Briceño, E. (2021). *Seguridad De La Información.* Alicante, España: Editorial Área De Innovación Y Desarrollo,S.L.

- Villalba-Fiallos, A. (2017). Reflexiones Jurídicas Sobre La Protección De Datos Y El Derecho A La Intimidad En La Autodeterminación Informativa. *FORO - Revista De Derecho*(27), 23-42.

- Zamudio-García, L. F. (2015). Tratamiento De Datos De Menores Y Políticas De Privacidad De Facebook. Colombia: Universidad De Los Andes.