PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE DERECHO Y SOCIEDAD

CARRERA DE DERECHO

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

TÍTULO

El valor probatorio de la prueba digital en el Código Orgánico General de Procesos

ESTUDIANTE: Yajaira Darnely Alvarez Bolaños

DIRECTOR: Mtr. José David Paredes Sandoval

Quito, D.M., 2024

Dedicatoria

A lo largo de este gran y largo camino, aprendí que los sueños y metas no se alcanzan en soledad, sino gracias al esfuerzo, amor y apoyo de quienes nos rodean.

Dedico y agradezco por la culminación de este trabajo, en primer lugar, a Dios, que me brindó, Fortaleza, sabiduría y resiliencia para afrontar cada desafío.

A mis padres amados, Jairo Alvarez y Darnely Bolaños, por su apoyo incondicional, su amor infinito, por ser mi guía y mi luz en medio de la tormenta, y por hacer de nuestro hogar un refugio de amor inquebrantable y de apoyo sin fisuras.

Al amor de mi vida, mis hermanas, Anita y Martina, mi mayor ejemplo a seguir, mi razón de ser y estar, gracias por nunca dudar de mi, y por hacer de mi existencia algo maravilloso, nosotras somos un para siempre.

A mis abuelitas, Hildita y Anita, el amor más puro y sincero que alguien ha podido entregar, donde su bendición siempre cargada de fe y amor fue mi protección frente a la adversidad.

A mi tutor de tesis José Paredes, mentor esencial en la formación de mi vida universitaria, por su acompañamiento constante, sus consejos y confianza.

Resumen

Al paso en que evoluciona nuestra sociedad, avanzamos nosotros por ser parte de ella e incluso la tecnología, el mismo que ha transformado ciertos elementos en la parte legal y judicial de nuestro país. Es por ello que, la digitalización trajo consigo diversos cambios en los procesos legales, claro está que estos cambios han sido tanto buenos como malos, ventajas considerables en el sentido de la celeridad en el ámbito del sistema de justicia del Ecuador. A pesar, de que el COGEP, añade en su normativa vigente como tal la prueba digital, el problema aquí es la ausencia clara y precisa de las directrices sobre su aceptabilidad y evaluación, creando de esta manera una confusión innata acerca de como se debe proceder. Esta falta de directrices puede traer consigo diferentes interpretaciones por parte de quienes están día a día en esa labor, primando así la imparcialidad y subjetivad. Es por esto por lo que, esta investigación tiene como objetivo determinar la validez y eficacia contar con parámetros claros de como abordar y proceder ante estas situaciones dentro de nuestro sistema judicial.

Es por ello que, uno de los desafíos mas importantes que se ha logrado encontrar es la falta de información y preparación certera de la persona que es se encuentra trabajando dentro de nuestros sistemas, lo que complica aun mas la efectividad de la digitalización en este sentido las pruebas en todos los procedimientos legales. Todo esto va a generar un síntoma de desconfianza en la sociedad hacia de cómo se maneja el sistema de seguridad y la celeridad y habilidad para tratar todo este tipo de casos en sociedad ya digitalizada, es por esto que, nos hemos visto en la necesidad de crear y suministrar mecanismos que puedan evitar la alteración de las pruebas y evidencias que se presenten, salvaguardando así sus derechos y la privacidad de cada persona.

Palabras Claves: COGEP; admisibilidad; valor probatorio; prueba

Abastract

Technological transformation has profoundly impacted the judicial sphere, introducing digital evidence as a new form of proof. This presents both opportunities and significant challenges for Ecuador's justice system. Although the Organic General Code of Procedures (COGEP) recognizes digital evidence, the lack of clear guidelines on its admissibility and assessment creates ambiguity. This normative uncertainty can lead to divergent interpretations, affecting impartiality and fairness in judicial proceedings.

This study analyzes the legal validity of digital evidence and its implications within the Ecuadorian judicial system. One of the main challenges identified is the insufficient infrastructure and lack of specialized training in digital matters among judicial personnel. This situation limits operational efficiency and could erode public trust in the system's ability to resolve complex cases. Therefore, it is crucial to establish mechanisms that guarantee the authenticity, integrity, and preservation of digital evidence through robust technical protocols, ensuring its proper management and legitimacy in judicial proceedings.

Keywords: COGEP, Admissibility, Evidentiary value, Evidence

Contenido

Introducción 7
1.1. Contexto y Justificación 7
Planteamiento del problema 9
Sección 1: Marco Teorico 11
1.1 Concepto de prueba 11
1.2 Concepto de Prueba en el Proceso Judicial 11
1.3 Digitalización en el procedimiento civil 12
1.4 Análisis de la prueba digital 13
1.5 Criterios de autenticidad de la prueba digital 19
1.6 Criterios de valoración de la prueba 25
Sección 2: Protección de datos 28
2.1. Mensaje de Datos 28
2.2 Manejo de la información de carácter personal: datos sensibles. 30
2.3 Riesgos asociados al tratamiento de datos sensibles 32
2.4 Limitaciones al consentimiento como fuente de legitimación 34
2.5 Tratamiento de datos personales dentro de un proceso judicial 34
2.6 Finalidad del tratamiento judicial de datos personales 35
Conclusiones/Recomendaciones 39
Bibliografía 42

Introducción

1.1. Contexto y Justificación

Los desarrollos tecnológicos han influido de manera significativa en el campo jurídico, particularmente en lo que se refiere al manejo de la evidencia digital. Es asi, que en el caso de Ecuador, el Código Orgánico General de Procesos (COGEP) establece un conjunto de normas que rigen la aceptación y valoración de este tipo de prueba, abordando los desafíos que surgen de esta nueva situación. Es por ello que, esta investigación va a determinar cómo se puede administrar y regular de una manera eficaz las pruebas digitales de conformidad con el COGEP, analizando principios, conceptos y de como se rigen al procedimiento probatorio, si está apegada a la realidad o no.

La era digital y la incrementación de la indumentaria tecnológica ha hecho que la prueba en formato digitalizado se convierta en algo sumamente necesario e importante a la hora de continuar con un proceso judicial, esto debido a que la facilidad ahora de mandar en un segundo dicha información genera un aceleramiento de todo este tipo de procesos. Eso sí, como lo abordábamos hace un momento genera cierta desconfianza porque todo este tipo de información se puede volver fácilmente manipulable, en el sentido de que se puede alterar su autenticidad. Por tanto, el COGEP nos facilita y suministra con normativa vigente para asegurar que la prueba sea pertinente, útil, conducente y legal. (Quchimbo Roman, 2024).

A medida que pasa el tiempo incrementa la tecnología y nosotros como sociedad avanzamos con ella en nuestra vida cotidiana, por eso se ha visto esta necesidad de adaptar el sistema en nos encontramos ya que estas expuestos a diferentes tipos de peligros cibernéticos. Claro está que, con ellos crearíamos nuevas posibilidades para acelerar y optimizar la eficacia del sistema jurídico, implementando retos a la hora de su aplicación y práctica ya que sin esto se verían vulnerado derecho esenciales de las personas.

Este estudio se centra en la premura de comprender como puede aportar la digitalización en el ámbito judicial, creando certeza y seguridad de que a la par se vayan respetando los derechos de todas las personas en un entorno totalmente digitalizado, de la misma forma, apegados a la realidad jurídica en la que vivimos adaptarnos a las normas implementadas por el COGEP, con este pretendemos crear una marco ya sea normativo vigente que se asegure la imparcialidad y la justicia en la digitalización de la prueba.

Por ello la adecuada aplicación de principios inherentes y básicos como la proximidad, oposición y la transparencia, es necesaria para asegurar un sistema y procedimiento judicial netamente justo. De la mano protocolos precisos sin vacíos normativos que se preste a diferentes subjetivas, asegura la legitimidad en nuestro sistema. La integración efectiva de la prueba digital promueve una gestión de la justicia más actualizada y eficaz. (Quchimbo Roman, 2024)

Objetivo General

Comprender y analizar de manera íntegra como la digitalización en general, conforme los parámetros aportados por el Cogep, perjudica o beneficia a la eficacia, eficiencia en la celeridad dentro de un sistema que aun no se encuentra totalmente digitalizado.

Este análisis engloba de manera detallada las consecuencias éticas, legales, jurídicas y normativas que nace con esta digitalización, con el objetico y meta de elaborar un marco normativo que plantee la seguridad, equidad y justicias específicamente en el tratamiento de la prueba.

Objetivos Específicos

Analizar de manera específica las normas del COGEP que abarca ciertos criterios de valoración de la prueba, haciendo un énfasis extenuante con la prueba física tradicional. Con este

análisis tendremos la oportunidad de verificar si efectivamente afecta al proceso como tal o lo beneficia.

Desarrollar y comprender las consecuencias legales debido a una pronta y acelerada digitalización en el proceso de valoración de la prueba, centrándonos directamente en como proteger los datos de las personas, la intimidad y la autenticidad al momento de entregar este tipo de información privada. Este estudio tiene como objetico la creación de mecanismos y acciones que aseguren la claridad de estas, así como, establecer los parámetros necesarios para no poner en peligro nuestros derechos y principios que nos rigen. Asimismo, se investigará los nuevos retos legales y técnicos que han emergido con la implementación de pruebas digitales y su repercusión en la administración de justicia.

Planteamiento del problema

La importancia y utilidad de este análisis se centra de comprender de ¿Cómo este avance tecnológico puede cambiar en nuestro sistema jurídico?, haciendo énfasis en una valoración ética, legal y social, es así que el núcleo de esta investigación se basa en la prueba digital dentro del COGEP, es por ello que, debemos estar sumamente consientes de las adversidades en las que nos encontramos ya sea para el beneficio de una pronta respuesta en un tramita como las desventajas que se adquieren en el proceso, como lo es la alteración de la prueba, presentando importantes avances y desafíos para su aplicación. (Piedra Iglesia, 2023)

Uno de los grandes desafíos a los que nos enfrentamos, que a pesar de que el COGEP, admite y esta consagrada en la ley las pruebas digitales, todavía no está reglada de manera adecuada y clara, creando confusiones y obstaculizando el cumplimiento a un certero debido proceso.

Por otro lado, la falta de preparación, lo lento que es nuestro sistema es de igual de cuestionable, como lo planteábamos en el apartado anterior la falta de infraestructura, de intentar tener un avance tecnológico ya sea en la preparación del personal como en la adquisición de implementos para esto, imposibilita una adecuada manera de trabajo rápido.

La interrogante legal que emerge de este análisis tiene como meta crear un marco para el examen crítico y la consideración sobre la manera de como optimizar las leyes y normativa vigente así como la implementación de la digitalización en el contexto de la prueba, garantizando que el sistema judicial de Ecuador pueda hacer frente de forma efectiva a los retos actuales. (Piedra Iglesias, 2023)

Sección 1: Marco Teórico

1.1 Concepto de prueba

Pero para entender este análisis planteado, es necesario primero comprender que es la prueba, ya que esta tiene numerosos conceptos y es entendida de diversas maneras, ya que esta está ligada estrechamente con la cotidianidad de las personas, es inherente a cada una de las actividades que realicemos en el día a día de una persona. Según (González, s. f.), el verbo "examinar" se refiere a comprobar o experimentar las características de personas o elementos, así como validar y demostrar la veracidad de algo. Asimismo, se destaca la diversidad de contextos en los que se aplica el concepto de evaluación, como en el ámbito educativo, donde un docente expone un tema y posteriormente comprueba los resultados al evaluar a sus estudiantes. De este modo, el término "validar" se vincula con el concepto de "aprobar" en este marco académico.

En base a esto, podemos comprender así que la prueba consiste en un conjunto de mecanismos creados y adoptados por la normativa que permiten que las partes que encuentra implicadas en algo puedan comprobar la veracidad de los hechos dentro de un proceso.

De conformidad con el artículo 160 del COGEP, la labor mas importante de la prueba como tal es ayudar o asistir al juez para la toma de una decisión sobre la veracidad de los hechos planteados y que estén a punto de determinarse, eso sí, deben ser pruebas contundentes cumpliendo ciertos requisitos, por ello, la prueba debe sestar dotada, de idoneidad, utilidad y exigencia apegada a la ley.

1.2 Concepto de Prueba en el Proceso Judicial

La prueba es un aporte importante y esencial dentro del sistema, puesto que asegura la claridad y veracidad de los hechos en los que estén implicados las partes. De conformidad con el COGEP, la prueba se describe como el conjunto de elementos que ayudan a evidenciar existencia

de un hecho que se encuentra en disputa por dos partes. De hecho, existen diferentes maneras de probar y evidenciar algo, por eso hay pruebas de diferentes tipos, tales como; testimonio, documentación, peritajes y por ende evidencias tecnológicas. Es por ello que se ha visto esta enorme necesitad de ir creando y modificando las leyes procesales para poder ir incorporando esta categoría digitalizada.

Es así que, al ir evolucionando, la tecnología transforma ciertos hábitos de la vida de las personas y no se diga en el ámbito legal, que, así como avanza la sociedad avanza el derecho,

Por ejemplo, en Ecuador, el COGEP ha suministrado ciertas directrices de cómo debemos abordar este tipo de pruebas en el ámbito judicial, creando ciertos desafíos. (Sacoto Romo, 2021)

1.3 Digitalización en el procedimiento civil

Es necesario abarcarlo en el procedimiento civil, ya que es un elemento crucial dentro de un proceso, y más ahora que han surgido ciertos delitos cibernéticos, una de las desventajas de estar cerca esta completa digitalización, es no saber a qué se está expuesto.

A pesar de que, el Código Orgánico Integral Penal y el Código Orgánico General de Procesos aceptan la legitimidad de la prueba digital, la ausencia de una adecuada y precisa regulación evita la correcta utilización por parte de nuestros jueces. Según (Bulnes, 2016) el objetivo de la prueba como tal digital netamente en la parte civil ha transformado retos y cambios importantes en la manera de como llevar un juicio, modificando el desarrollo de cómo se los planteaba, esto debido a que ahora existen contratos electrónicos, totalmente digitalizados, intercambios digitales, pautas tecnológicas y operaciones realizadas en plataformas en línea.

Es por ello que este análisis evidencia estos problemas actuales en los que nos estamos enfrentando porque que tan veraz resulta algo que se ha pactado de manera digital y como se puede comprobar que no está alterado su autenticidad.

Al contrario de lo que tenemos que son las pruebas físicas tradicionales que se cuenta con un soporte netamente tangible, a diferencia, de los documentos en formato electrónico carecen de un soporte material, lo que se necesita de una normativa que acredite y asegure la privacidad de las personas. Pero no por esto, debemos dejar pasar el tiempo y estancarnos, tenemos que modernizarnos y crear diferentes mecanismos de apoyo para regular este tipo de situaciones.

Una parte esencial de esta investigación, es la valoración de la prueba digital, por tanto, es importante que las partes sean totalmente honeste y no generen alteraciones en las pruebas que se intenta evidenciar algo, que su origen sea completamente veraz y original. Es por ello que se han creado los peritos informáticos, expertos en la digitalización y autenticidad de la información que se ha presentado.

Es por ello, que se evidencia directamente cuando el juez debido a la falta de leyes concretas y claras puede determinar algo erróneo, provocando una inseguridad tremenda dentro de la sociedad, ya que no se tiene conocimiento de si esa información brindad no fue alterada, y más en juicios civiles, ya que la autenticidad no es fácil de comprobar.

Es por esto, que es importante abarcar y encontrar una línea balanceada entre de como sed debe adaptar esto sin afectar derechos inherentes y fundamentales de las personas, la validación que se le dé a una prueba digitalizada debe poder ser cuestionada por la otra parte, por lo que es crucial que el juez evalúe de forma justificada su relevancia, idoneidad y veracidad.

1.4 Análisis de la prueba digital

La evolución de las tecnologías en el ámbito de cómo se puede enviar cierta información ha creado un cambio significativo en la manera en que se crea, guarda, envía y se muestra la

misma. Es por ello, que en la parte legal no ha sido una excepción y se cree que es uno de lo mas afectados. En este contexto contemporáneo, aparece la prueba digital, un tipo de prueba cuya esencia, utilización y valoración generan ciertos problemas jurídicos y legales importantes dentro de la normativa en una sociedad, (Quchimbo Roman, 2024)

A pesar de que, en nuestra legislación específicamente en el COGEP no nos suministra de un concepto preciso de lo que es una prueba digital y tecnológica como tal, si nos proporciona en general que la prueba debe estar dotada de ciertos principios, como de utilidad, legalidad y adecuación al momento de presentarla. Por eso este instrumento digital puede ser utilizado como prueba siempre y cuando cuente con que sea totalmente verificable y tenga total relevancia con los hechos en particular.

De hecho, la prueba digital es aceptada como un mecanismo tecnológico que comprende información detallada que puede ser analizada por los jueces. Dicha información, al ser accesible de manera tecnológica esta al alcance de cualquier persona, requiere de autenticidad, facilitando su comprobación dentro de un proceso. De conformidad con el artículo 202 del Código Orgánico General de Procesos, se acete y permite que toda información electrónica y mensajes, cumplan y estén dotas de idoneidad y autenticidad (Vera Quezada, 2024)

Es así que, el ámbito penal, específicamente en Código Orgánico Integral Penal (COIP), se permiten la prueba digital facilitando su uso, debido que la creación de ciertos delitos digitales ha creado esta necesidad de hacerlo. De conformidad con el artículo 500 numeral 2 del COIP en el que establece; “Toda evidencia digital o electrónica será válida siempre que se obtenga de forma legal, se garantice su integridad, autenticidad, cadena de custodia y posibilidad de contradicción.”

Podríamos analizar que esto efectivamente implica que la admisibilidad y el valor probatorio de la prueba digital dependen de ciertos requisitos, que aseguren su origen auténtico y que no haya sido modificada. Es por ello que la regla solicita asegurar aspectos fundamentales como:

Legalidad en la obtención: Esta debe ser recolectada principalmente sin vulnerar derechos constitucionales, especialmente el derecho a la privacidad y al debido proceso.

Autenticidad e integridad: Este es de suma importancia debido a que se debe demostrar que el archivo no ha sido manipulado desde su origen.

Cadena de custodia: Aquí es relevante mantener un registro continuo y documentado del manejo de la evidencia desde su recolección hasta su presentación en juicio. Es importante manifestar que tanto dentro del COGEP y de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos no se cuenta con la cadena de custodia lo cual complica este registro.

Contradicción: El principio en que las partes deben poder impugnar y contradecir la prueba durante el juicio.

Y por último, tenemos que analizar la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, refiere a prueba digital a toda aquella información de formato electrónico que sea de útil en el proceso legal, ya sean mensajes de datos, correos electrónicos, firmas, etc. De conformidad al Art 2 de la LCE:;

"*Se reconoce la validez jurídica de los mensajes de datos y de las firmas electrónicas, otorgándoles los mismos efectos que los documentos escritos y firmas manuscritas*"

Sin embargo, como se discutió en la sección anterior, para realizar un análisis exhaustivo necesitamos considerar ciertos criterios y entender las diferencias que surgen al hablar de lo mismo tanto en el ámbito digital como en el físico. Esto se debe a que, según el COGEP, la

prueba se define como el conjunto de medios que son legalmente aceptados, permitiendo que las partes confirmen la veracidad de los hechos en un juicio. De acuerdo con el artículo 160 del COGEP, su propósito es ayudar al juez a tener una convicción sobre la verdad de los hechos en conflicto. Por otro lado, en el COIP, "La prueba busca convencer a quien juzga sobre los hechos y circunstancias involucrados en la infracción y la responsabilidad del acusado". Si analizamos esto desde la perspectiva de la Ley de Comercio Electrónico en relación con las Firmas y Mensajes de Datos, la prueba se interpreta como el conjunto de medios y documentos electrónicos que se emplean para validar la existencia, validez y contenido de un acuerdo o contrato realizado a través de medios electrónicos.

Después de haber comprendido, como se aneja la valoración de la prueba dentro de los diferentes marcos normativos, podemos manifestar que la prueba es un componente sumamente importante en cualquier proceso, debido a que, a través de esta se pretende materializar la veracidad de diferentes hechos que se encuentran en discusión. Pero nos pudimos dar cuenta, que el manejo, el concepto y su utilización es completamente diferente en la normativa vigente de nuestro país, esto ya que, se apega a la necesidad de lo que se está viviendo.

Es por ello, que es relevante investigar de manera detallada como se aborda en almenos tres de nuestra legislación, para así comprender como ser percibe la prueba en nuestra sistema. Tanto es el Código Orgánico General de Procesos (COGEP), el Código Orgánico Integral Penal (COIP) y la Ley de Comercio Electrónico, Firmas y Mensajes de Datos.

Podemos iniciar entonces con el COGEP, que este se encarga netamente de procesos allegados de naturaleza civil, familiar e incluso administrativo. En concordancia con el artículo 160,en donde manifiesta la admisibilidad de la prueba, y de como se la debe presentar dotada de todos los criterios y principios clave para que pueda ser admitida. Añadiendo de que no esta

permitido presentar una prueba que contenga malicia o dolo, claro está hablando en términos generales, ya que hablando de una digitalización no se encuentra como tal normada.

De hecho, la función que tiene el COGEP en el ámbito de la prueba, es completamente allegada a los derechos de las personas es garantista y procesal. Ya que, no solo se restringe, a como se debe presenta una prueba, sino también vas más allá de que realice bajo principios en donde no vulnere derechos fundamentales de las personas, esto es, en que se asegure de que todo el proceso será legal y justo.

Al contrario del, COIP, que regula completa,nete todos los procesos penales de una persona, este tiene una idea mucho más estricta, rígida y finalista sobre la presentación de la prueba. En este marco normativo lo importante es la veracidad y la existencia de una prueba y de que la personas a la que se la está acusando dependiendo las pruebas en que se hayan presentado sea determinado culpable o pueda ser libre. A diferencia de como notamos en el marco legislativo civil, donde puede incluso caber una duda razonable, en el ámbito penal, esto no puedo caber ya que existen ciertos principios como la es la presunción de inocencia y de la prueba debe ir mas allá de toda duda razonable, por ello la presentación de la prueba al momento de determinar algo que se encuentre en disputa debe ser totalmente rigurosos.

Finalmente, la Ley de Comercio Electrónico, Firmas y Mensajes comprende un concepto mucho más allegado a lo que es una prueba digital, abarcando como tal la transformación de esta era informática, a las nuevas formas de como se pueda ahora manejar la digitalización, de ciertos tipos de contratación y comunicación. Este marco normativo, permite los mensajes de datos, información digitalizada etc.

La finalidad de esta legislación va más allá de como se debe presentar una prueba y bajo que criterios, porque eso lo tenemos en el COGEP, este se centra mas en la posibilidad de brindar

apoyo y seguridad al momento de que la autenticidad de una prueba digital haya sido afectada, garantizando de esta manera la privacidad de todas las personas.

Podemos concluir, que estos tres marcos normativos se apegan a la realidad de la que estamos viviendo, y de que todos aportan un importante papel dentro de nuestra sistema judicial, pero que es evidente la manera en que cada uno lleva un proceso totalmente diferente, es así que, el COGEP es totalmente procesalista se lleva más acabo la menra en como se la debe presentar, el COIP un tanto más riguroso, protegiendo derechos inherentes y fundamentales dentro de la responsabilidad penal que se tenga en ese momento. Por otro lado, la Ley de Comercio Electrónico que comprende un poco más esta realidad virtual que acecha a la sociedad, y determina y garantiza de una manera mas aproximada la prueba digital.

Es por esto, que este investigación nos permite entender como el derecho está obligado a evolucionar y transformar todo su marco legal a medida de que la sociedad y las personas cambian.

Por lo tanto, podemos afirmar que esta transformación es realmente importante abarca ciertos principios de facilidad, así como el de celeridad para poder optimizar de manera rápida y eficaz ciertos procesos judiciales, así se podría verificar la autenticidad de una prueba digital, una firma digital un mensaje de datos etc. Sin dejar de lado esta inseguridad constate de como evoluciona este tipo de información, de como se puede salvaguardar nuestros derechos y la integridad y privacidad de cada una de las personas.

Al contrario, de la prueba que tiene un soporte físico o material,

Aunque con esto no es que asegure de que evidentemente no pueda ser alterada, siempre ha estado en nuestra legislación y por eso cuenta con un marco legislativo mucho más apli, claro y preciso de cómo se debe manejar y aceptar.

Para finalizar, esta incorporación requiere de mejores procedimientos, de diferentes transformaciones en la legislación, de un mejoramiento pronto y necesario de todas las leyes vigentes que encuentra en nuestro país.

1.5 Criterios de autenticidad de la prueba digital

En todo lo que va de la investigación hemos hecho hincapié en que la prueba debe dotar debe autenticidad, es por ello que es importante abarcar su concepto y para que sirve. La autenticidad se refiere específicamente a la garantía de que todos los componentes de la prueba son verificables y de que adolecen de cualquier tipo de adulteración.

Es así que está ligada completamente a la cadena de custodia, que incrementa y verificada cada detalle desde el momento en que ha sido recolectada hasta la presentación de esta. (Vera Quezada, 2024)

En la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (LCEFM) se identifica la autenticidad en la veracidad de mensajes de datos y firmas electrónicas haciendo un balance con las de soporte físico y esta claramente sustentada dentro de ciertos artículos y para mayor entendimiento serán explicados.

Artículo 2: se puede evidenciar la urgencia **y** necesidad de conferir el mismo valor probatorio que cualquier otro de soporte físico, verificando s veracidad y fiabilidad.

Artículo 6: En este, consagrada el concepto de que puede acreditarse siempre y cuando se mantenga la integridad y veracidad del mismo y de que provenga de un emisor identificado.

Aunque la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (LCEFM)

Da validez jurídica a la prueba de soporte electrónico, ya sea como mensajes de datos y firmas, no hace referencia a la urgencia de determinar una cadena de custodia netamente digital que como ya conocemos este permite y asegura la integridad, veracidad y autenticidad de cualquier tipo de información digitalizada, desde la recolección hasta la presentación de la misma. (Parra, 2019).

Es por ello, que la falta de una legislación propicia y adecuada dentro de un sistema constata la negativa de no hacer ciertos cambios, es por ende que es sumamente importante evidenciar su autenticidad para que el juez pueda determinar de manera precisa lo que se le está pidiendo y de que pueda crear una convicción apega a la realidad y la ley.

En lo que pasa día a día la información digitalizada puede ser alterada y manipulable de forma sencilla, sin embargo, el problema sería de darnos cuenta de este tipo de indicios y de que se pueda detectar de una forma rápida e inmediata, es por ello que la creación de la cadena de custodia es sumamente importante porque agilizaría los proceso y así también salvaguardaría desde su recolección no dejando paso a cualquier tipo de alteración. (Financial Crime Academy, 2024).

Hablando de derecho comparado es necesario manifestar que en marcos legislativos europeos o incluso en Colombia, se encuentran mucho más modernizados y digitalizados, apegados a la realidad que se vive en este momento, es por ello que han creado ciertas maneras de custodiar la prueba digital, al contrario de lo que nos pasa en Ecuador que nos encontramos completamente limitados a la custodiabilidad de una prueba digital.

Por ejemplo, en Colombia, el Código General del Proceso ha establecido cierto parámetros para la prueba digital, lo que ha incrementado su agilidad y eficacia dentro de sus procesos legales, así como también la seguridad y privacidad de sus ciudadanos, enmarcando la

necesidad de contar con una cadena de custodia , es así que, en el caso de Ecuador, la ausencia de normativa vigente que incluya la digitalización obliga a que la responsabilidad dependa netamente de informes digitalizados o la perspectiva del juez, lo que claramente genera subjetividad y ambigüedades a la hora de resolver ciertos casos, lo que se estaría afectando directamente derechos y principios procesales importantes. (Quchimbo Román, 2024).

Por lo tanto, aunque como revisamos en el articulo 2 la LCEFM en donde manifiesta esta necesidad de equiparar a los mensajes electrónicos con cualquiera de otro tipo de soporte físico, no se podría generar un cierto balance entre ambos porque a pesar de que este equiparado se necesita de una regulación pronta, precisa y adecuada.

Es por ello, que esta falta de cadena de custodia queda en total arbitrariedad y pueda ser rechazada por el juez, o lo que es peor aún que sea aceptada sin que se cuente con los requisitos de autenticidad al momento de verificar su origen.

Esta urgencia, necesidad y carencia legal requiere de una transformación vital en nuestros cuerpos normativos, enfocadas la creación de directrices adecuas a la aplicación de la cadena de custodia, esto alineado claramente con estándares y jurisprudencia internacional de aplicación en la prueba digital.

La legislación ecuatoriana sobre Comercio Electrónico, Firmas y Mensajes de Datos define las normas básicas que rigen la creación, conservación y comprobación de la evidencia digital, aceptando su validez legal igual a la del documento físico. En relación a su creación, la normativa se basa en el reconocimiento de los mensajes de datos como pruebas legítimas, siempre que provengan de medios electrónicos seguros. El artículo 2 de la ley señala que se otorgará a los mensajes de datos y a las firmas electrónicas *“los mismos efectos que los*

documentos escritos y firmas manuscritas", permitiendo así la creación de contratos, notificaciones, declaraciones y demás actos jurídicos a través de medios digitales.

En cuanto al almacenamiento, la normativa indica que los mensajes deben ser guardados de manera completa y que sean accesibles para futuras consultas. Es por ello, que en concordancia con el artículo 9 aclara que se considera que se cumple con el requisito legal de tener un documento escrito cuando la información del mensaje de datos puede ser revisada más adelante sin modificaciones. Además, es necesario citar el artículo 11 debido a que este establece que para que un mensaje tenga validez como prueba, debe conservarse en un formato que mantenga su contenido original, junto con metadatos clave como el origen, la fecha de envío o de recepción, y, si es factible, un registro técnico verificable, como huellas digitales o sellos de tiempo. Esta normativa, aunque es esencial, no cuenta con una guía técnica específica que defina los métodos obligatorios para esa conservación.

En resumen, aunque la LCEFM constituye un progreso en el reconocimiento de la evidencia digital, la falta de una normativa técnica específica acerca de su custodia, conservación y reproducción restringe su capacidad probatoria completa. Esta carencia en la normativa necesita ser atendida con regulaciones adicionales o modificaciones en el marco legal, que ofrezcan criterios claros para el manejo seguro y verificable de la prueba electrónica en los juicios en Ecuador. (Quchimbo Román, 2024; Parra, 2019).

El Código Orgánico General de Procesos (COGEP), como abordamos y sabemos esto solo se basa en procesos netamente civiles, familiares o laborales, aunque si permite el uso de documentos digitales y lo hace válido, pero lo determina de una manera muy amplia y genérica. Por eso que dentro de nuestro sistema este principio es de suma importancia debido a que, genera un cierto grado de comprobación veraz,

En el artículo 202 del COGEP, se determina que podrán ser presentados y aceptados adecuadamente documentación digitalizada, siempre y cuando cumplan con todos los requisitos establecidos por la ley, esto es criterios de autenticidad, Sin embargo, a pesar de que en la norma se encuentra validado esto, es imposible determinar las directrices que se deben utilizar para poder validar lo autentico de dicha prueba, ni tampoco como se debe llevar un proceso para validar su integridad. Es por ello, que esto queda en total convicción de lo que el juez haya podido determinar, y lo que las parte dentro de eso proceso hayan podido comprobar, generando así cierta arbitrariedad y subjetividad a la hora de resolver ciertos parámetros importantes en un caso.

Al contrario, de lo que pasaría con material totalmente físico, que se lo puede adulterar, pero su descubrimiento de eso sería mucho más sencillo, en cambio, en la prueba digital como se puede verificar si ha siso alterado o no, requiere de un análisis más exhaustivo que contenga metadatos, cadenas de digitalización seguras, etc.

Además, el artículo 160 del COGEP promueve que la prueba que este en disputa en ese proceso, de conformidad con los principios de legalidad, utilidad y relevancia se cree una convicción veraz y necesaria. Es por ello que, se ha podido deducir que efectivamente hace falta de directrices legales, para analizar y comprobar cierta autenticidad.

En diferentes ocasiones, las partes ven la necesidad de acudir a ciertos informes digitales, en el que su costo puede ser sumamente elevado, generando así una afectación a derecho y principios fundamentales.

Al momento de presenta una prueba digital los requisitos son sumamente ambiguos, ya que no se presenta con claridad sobre el formato en que este debería ser presentado, creando así otra desventaja en la celeridad de un proceso.

Podemos concluir, que aunque existe tal vez una determinación y un concepto de la prueba digital, se nota la carencia de esta aceptación formal, dejando normas técnicas sueltas sin saber cómo aplicarlas, ya que no se podría evidencia su almacenamiento, originalidad, creación, incluso el formato de cómo se debería presentar.

Por lo tanto, es sumamente importante la transformación y modernización de nuestros cuerpos normativos que definan conceptualicen de manera clara y precisa el procedimiento y de como se debe llevar a cabo acelerando y facilitando su aplicación.

Sin embargo, según UCTunexpo (s.f.), para contrarrestar la carencia de una cadena de custodia que asegura a la prueba desde la recolección hasta la presenta dentro de un proceso, el COGEP introdujo de manera precisa la necesidad de arraigarnos al principio de comunidad probatoria, o también conocido como principio de adquisición, pero que es este principio, es básicamente esta necesidad de que en el momento exacto en que se encuentre incorporada la prueba dentro del proceso se convierte en parte del mismo y no de la persona de la que presentó, sino que va al acervo común del proceso en cuestión, beneficiando de esta manera a cualquiera de las dos partes, independientemente de quien la haya presentado. La manera en como se aplica este principio resulta propicio para todas las partes incluyendo al juez debido a que el juez puede encontrar las pruebas a la mano y de manera más rápida facilitando los resultados del proceso.

En función de lo mencionado, no está permitido que las dos partes, en preciso momento puedan presentar la prueba, o desistan de la misma, porque ya se encuentra dentro del acervo común del proceso.

Es por eso que este principio va de la mano con el de oportunidad y de contradicción ya que estos garantizan el derecho propicio a la defensa.

Desde esta perspectiva, este principio actúa fundamentalmente como un sistema de purificación de procesos, que contribuye a mantener tanto la eficacia como la eficiencia de las pruebas derivadas de esos datos digitales cuya cadena de custodia no se haya verificado de manera fidedigna. Por supuesto, este contenido no debe haber sido cuestionado previamente por la parte opuesta.

No obstante, este criterio relacionado con la comunidad no puede ser invocado si presenta arbitrariedades tales como violaciones de cualquier tipo. De hecho, esto incluye el debido proceso, especialmente cuando la evidencia se obtuvo de manera ilegal o en contravención de derechos fundamentales. En tales circunstancias, la exclusión de pruebas es prioritaria respecto a la obtención procesal. De manera similar, en el ámbito penal, donde prevalece el principio de presunción de inocencia y la necesidad de pruebas sin lugar a dudas, la jurisprudencia ha restringido la aplicación de este principio ante la falta de cadena de custodia, debido a la demanda más rigurosa en la evaluación de pruebas digitales.

En la teoría comparativa, pensadores como Michele Taruffo y Francesco Carnelutti manifiestan que estos principios funcionan y fortalecen al proceso y al conocimiento de lo que existe, acercándolo aun mas a una verdad procesal mucho mas cercana a los hechos.

1.6 Criterios de valoración de la prueba

Dentro del ámbito legal, uno de los objetivos del juez es determinar con verdad lo que ha sucedido sin embargo, también es una de las partes más difíciles debido a que, al momento de determinar el valor probatorio si no se tiene las pruebas necesarias se complica aun más.

El COGEP indica que para no llegar a este punto es necesario hablar de criterios racionales, para poder resolver diferentes tipos disputas entre las partes dentro de un proceso

judicial, es así que, no solo requiere de que la prueba cuente con los requisito y esté dentro de un expediente, sino que también es necesaria la valoración, razonamiento y experticia dentro del mismo, por lo que podemos decir, que no es que se pueda presentar una prueba y ya y aceptar lo que diga un documento, sino determinar por que esa prueba en concreto es necesaria para dicho caso.

Esto es importante debido a que, en el mundo en que nos encontramos ahora, resulta o estamos mas limitados en determinar y analizar la autenticidad de un formato digitalizado, como lo es un mensaje de WhtasApp, un correo electrónico o PDF. Incluso a pesar de que en el COGEP en su artículo 196 detalla el procedimiento a evaluar una prueba digital en audiencia, se podría considerar que ciertos criterios todavía no están desarrollados de manera precisa y clara.

De acuerdo con José Luis Mazón, en su obra *Ensayos Críticos del COGEP*, menciona que este tipo de evaluación requiere que el juez profundice más allá de lo obvio. En el caso de pruebas electrónicas, no es suficiente con observar el material; es crucial entender su origen, si existió la posibilidad de que alguien lo modificara y si la otra parte tuvo la oportunidad de debatir sobre ello. Esto convierte el examen de pruebas en contextos digitales en algo más difícil, pero a la vez más indispensable.

Aquí entra en acción otro concepto que no siempre se menciona de manera directa en la normativa, pero que es bastante común en la práctica: el concepto de comunidad de pruebas. Esto implica que, una vez que una evidencia se introduce en el procedimiento y es accesible para ambas partes, ya no es exclusiva de quien la presentó. Se convierte en un elemento del proceso y puede ser empleada tanto en beneficio como en perjuicio de cualquiera de las partes.

Esto resulta particularmente beneficioso en situaciones donde se introducen pruebas digitales que carecen de ciertos requisitos técnicos ideales, como la cadena de custodia. Por

ejemplo, si una persona presenta una captura de pantalla de un chat de WhatsApp y la parte contraria no la impugna a tiempo, o incluso hace comentario al respecto durante la audiencia, el juez podría considerarla como admisible. A pesar de que esta evidencia pueda presentar fallos formales, lo fundamental es que haya sido reconocida, discutida y que no se haya infringido el derecho a la defensa. Mazón (2021) señala que esta forma de razonamiento está dirigida al propósito fundamental del proceso: encontrar la verdad de los acontecimientos. No es cuestión de triunfar mediante una artimaña legal o de sacar ventaja de un fallo técnico, sino de proporcionar al juez los recursos imprescindibles para emitir un fallo equitativo. De esta manera, la evaluación objetiva y el principio de comunidad de pruebas contribuyen a que la justicia abarque no solo aspectos superficiales, sino también cuestiones sustanciales.

En resumen, al referirnos a la evidencia digital, estos dos conceptos permiten que el juez evalúe de manera razonable lo que se presenta ante él, aun cuando no todo esté completamente respaldado desde el aspecto técnico. Por supuesto, esto no significa que se acepten pruebas que hayan sido alteradas o que sean ilegales. Sin embargo, implica que, cuando hay buena fe en el proceso y las evidencias han sido debatidas entre las partes, es legítimo otorgarles el peso adecuado, independientemente de los requisitos formales.

Sección 2: Protección de datos

2.1. Mensaje de Datos

Después de haber tratado todas las herramientas fundamentales y los criterios de evaluación de la prueba digital, es crucial comprender la importancia del mensaje de datos y su significado. Conforme al COGEP, aunque no existe una definición precisa, se considera que el mensaje de datos abarca diferentes formas de información, ya sea que haya sido creada, manipulada, concebida, generada, enviada, recibida o almacenada a través de cualquier tipo de medio electrónico.

Sin embargo, para explicarlo en mayor profundidad, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos establece un concepto muy relevante para garantizar que la documentación digital sea equivalente a la que se encuentra en soporte físico tradicional. Según el artículo 7 de esta ley, un mensaje de datos debe satisfacer ciertas condiciones, entre ellas que la información mostrada debe poder ser preservada en su estado original, siempre y cuando se pueda comprobar completamente la integridad de los datos desde el instante en que fueron introducidos. Esta norma acepta que no es la forma física del documento la que le da validez legal, sino su habilidad para mantener el contenido total y sin cambios, incluso si hay alteraciones inherentes al proceso de comunicación, almacenamiento o exhibición.

En esta regulación se puede observar igualmente cómo se lleva a cabo la eliminación del formato físico de documentos que legalmente necesitaban un soporte material convencional, esto debido a que, bajo las mismas condiciones de contar con firmas electrónicas validadas por las autoridades o las entidades correspondientes y de respetar los criterios de conservación fijados por la ley. Por lo tanto, el mensaje de datos tiene plena validez como evidencia documental, cuando se asegura su seguimiento, autenticidad y preservación.

En la misma línea, se puede señalar que el artículo 8 describe el procedimiento que se debe seguir para adquirir criterios de conservación que sean legalmente apropiados. Este procedimiento debe contener información que sea fácil de consultar en el futuro, preservando así su estado original. De este modo, se asegura que la información añadida se mantenga conectada a su origen, creación y destino para el envío y archivo. Además, se subraya la importancia de garantizar la integridad del mensaje durante todo el tiempo que lo requiera la normativa vigente. También se permite que esta conservación se delegue a terceros con experiencia, siempre que se cumplan los requisitos legales establecidos.

Sin embargo, es importante manifestar la transformación que ha representado un mensaje de datos a medida de que pasa el tiempo y en diferentes legislaciones, y se lo puede analizar de diferentes maneras e incluso en diferentes legislaciones, es por ello que en el ámbito empresarial, ha generado una modernización digitalizada en la tecnología,

En países como México, el mensaje de datos tiene relevancia debido a que estos pueden tener efectos legales, equiparados a un soporte tangible o material siempre y cuando se puedan respetar los principios básicos.

Adicionalmente, se resalta la función reguladora de normas técnicas como la NOM-151 en México. Para explicarlo de manera sencilla, este fue creado esencialmente para asegurar y preservar los mensajes de datos, creando así protocolos y directrices, lo cual implicaría una modernización dentro de su legislación, claro está que nosotros como país no contamos aun con ese tipo de parámetros para salvaguardar la privacidad y autentificación de los mensajes de datos, pero podríamos tomar en cuenta para crear un diferente tipo de modelo que sirva como guía para resguardar los datos. (DocuSing, 2022)

De esta manera, el mensaje de datos no se considera únicamente un recurso técnico, sino una base fundamental para el nuevo entorno legal y comercial. Su uso adecuado permite a los profesionales del derecho y a las empresas funcionar de manera efectiva y segura, sin perder las protecciones legales que caracterizan a los sistemas convencionales. (Mifiel, 2023)

2.2 Manejo de la información de carácter personal: datos sensibles.

A medida que la sociedad evoluciona y avanza, específicamente en lo que respecta al progreso tecnológico actual, se ha observado un rápido crecimiento en la recopilación, procesamiento y distribución de la información de cada individuo. Esto se debe a que, todos estamos involucrados en las redes, lo que hace que nuestros datos circulen por la esfera digital. Por ello, se vuelve fundamental proteger mis datos e información, ya que esta situación ha llevado a los gobiernos a establecer leyes y normativas específicas y especializadas para regular cómo se maneja esta información.

Es por ello que la Ley Orgánica de Protección de Datos Personales (LOPDP), que fue publicada en el Suplemento 459 del Registro Oficial el 26 de mayo de 2021, aquí podemos encontrar la conceptualización e incluso el proceso a llevar a cabo de la mano de principios y responsabilidades que rigen este tipo de manejo de datos, que van de la misma línea a marco normativos internacionales el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Es por ello que, tanto esta ley como el RGPD admiten que los datos personales considerados sensibles necesitan de una protección adicional debido a su particular capacidad de impactar en los derechos de los individuos.

Pero para lograr esto, es esencial entender de manera sencilla qué se entiende por un dato personal. La LOPDP suministra información en la que describe al dato personal como cualquier información que puede elaborar una persona o individuo de manera directa o indirecta.

Este concepto determinar que puede ser información completamente básica (como nombre, número de identificación, correo electrónico) hasta información sumamente privada como lo son las ubicaciones o las comras que se pueden realizar de manera digital, etc.

A diferencia de la información confidencial, esto abarca un tema o tipo de información que claramente debe manejarse de manera diferente por su carácter sensible. De acuerdo con el artículo 4 de la LOPDP, se clasifican como sensibles aquellas informaciones que, por su esencia íntima o que su uso incorrecto podría causar discriminación o daños severos a los derechos básicos de las personas, como se mencionó, estos requieren un manejo extremadamente cuidadoso, debido a su relevancia y la seriedad de la situación. Algunos ejemplos de esto podrían ser;

- Datos de salud física o mental;
- Datos genéticos o biométricos;
- Convicciones religiosas, filosóficas o morales;
- Opiniones políticas o afiliación sindical;
- Orientación sexual;
- Información sobre antecedentes penales.

Como podemos notar, todos estos ejemplos manifiestan datos complejos y personales de cada individuo, lo que implica que aborda temas serios. Su manejo, aunque pueda ser viable desde un punto de vista técnico o permitido en algunas situaciones, debe considerar ciertos principios y derechos esenciales, tales como; la necesidad, un objetivo legítimo, la reducción de datos y, sobre todo, la proporcionalidad.

2.3 Riesgos asociados al tratamiento de datos sensibles

Para todo lo mencionado, hay opciones alternativas cuando se presenta un uso excesivo del manejo incorrecto de información o datos personales sensibles, lo que puede llevar a consecuencias que, en algunos casos, son irreversibles. En nuestro marco legal, la Ley Orgánica de Protección de Datos Personales (LOPDP) define responsabilidades concretas para aquellos que manejan estos datos, las cuales deben ser tratadas en conjunto con medidas de ciberseguridad que garanticen la privacidad, integridad y accesibilidad de la información.

De conformidad con el artículo 37 de la LOPDP establece de manera precisa que aquellos que manejen información personal deben llevar a cabo prácticas técnicas y organizativas apropiadas para asegurar su protección. Es por esto que, esta responsabilidad se vuelve aún más crítica y estricta cuando el manejo incluye datos sensibles, que son aquellos que exponen facetas privadas o que podrían causar discriminación hacia el individuo.

El artículo 40 de la LOPDP requiere que las entidades lleven a cabo un análisis de riesgos relacionado con el manejo de datos personales, con el fin de identificar debilidades, amenazas y aspectos críticos del sistema de protección. Por ello, esta obligación es especialmente importante cuando se trata de datos sensibles, ya que el nivel de daño posible en caso de una violación es mayor. Un descuido en la gestión de estos datos puede resultar en consecuencias graves para los derechos de los titulares, como la discriminación laboral, la exclusión financiera, y el impacto psicológico o social, entre otros. Cuando el manejo de datos sensibles representa un riesgo significativo para los derechos de los individuos, el artículo 42 de la LOPDP requiere que se realice una Evaluación de Impacto en la Protección de Datos (EIPD). Esta herramienta sirve para anticipar, prevenir y corregir posibles situaciones de daño.. (World Complince Assosiation, 2023).

Tanto el sistema legal de Ecuador como el de Europa han incluido la regulación de la información personal, en especial la de carácter sensible, en el contexto de los derechos fundamentales. La capacidad de decidir sobre la propia información, que proviene del derecho a la privacidad, da a las personas la opción de elegir qué datos quieren dar, a quién, con qué propósito y bajo qué circunstancias.

En nuestro ordenamiento jurídico, este derecho se encuentra claramente mencionado en el artículo 66, inciso 19, de la Constitución, que asegura la protección de los datos personales. Dentro de este contexto, la Ley de Protección de Datos Personales (LOPDP) define varias condiciones particulares para el manejo de datos sensibles, entre las que se pueden resaltar:

- Consentimiento expreso y por escrito del titular;
- Finalidad determinada, legítima y explícita;
- Prohibición de utilizar los datos con fines distintos a los informados;
- Implementación de medidas de seguridad reforzadas;
- Evaluaciones de impacto cuando el tratamiento implique alto riesgo.

El Reglamento General de Protección de Datos (RGPD) indica que, en general, el manejo de datos sensibles está prohibido, a menos que se cumplan algunas de las excepciones claramente mencionadas en el artículo 9 de este mismo reglamento, tales como el consentimiento claro, razones de importancia pública fundamental o propósitos relacionados con la medicina y la salud pública.

Ambas regulaciones, en consecuencia, coinciden en afirmar que la información sensible debe recibir una protección especial, no solo debido a sus particularidades técnicas, sino también

por el significativo valor simbólico y legal que tienen en relación a la autonomía, la privacidad y la libertad.

2.4 Limitaciones al consentimiento como fuente de legitimación

Aunque el consentimiento es frecuentemente visto como el fundamento principal que legitima el manejo de datos personales, en lo que respecta a datos sensibles, esta fuente presenta ciertas restricciones que necesitan ser consideradas. Es importante señalar que el consentimiento debe ser voluntario, concreto, consciente y claro, lo que no siempre se cumple en situaciones donde hay desigualdad de poder (por ejemplo, entre un jefe y un empleado, o entre un paciente y un proveedor de salud).

Además, se puede retirar el consentimiento en cualquier momento, lo que requiere que quienes manejan los datos cuenten con procesos bien definidos para gestionar esa cancelación. Es así que, en situaciones como las plataformas en línea, donde el lenguaje de los términos y condiciones frecuentemente resulta confuso o ambiguo, el consentimiento informado puede convertirse en una ilusión legal si no se aplican medidas que faciliten la comprensión y el acceso.

Por lo tanto, aunque el consentimiento se mantiene como una base legítima, no debería verse como la exclusiva ni la más robusta en cada situación. Asimismo, en la gestión de datos delicados, es recomendable contar con fundamentos legales definidos, sistemas de supervisión institucional, directrices de conducta específicas del sector y un enfoque de cumplimiento activo por parte de quienes realizan el tratamiento.

2.5 Tratamiento de datos personales dentro de un proceso judicial

Normalmente, decimos que el consentimiento es la clave para usar los datos personales de forma correcta. Pero cuando hablamos de datos más delicados o sensibles, el consentimiento

no siempre es suficiente y tiene sus problemas. Para que un consentimiento sea válido, tiene que ser dado de forma libre, específica, informada y clara. Esto es muy difícil de conseguir cuando hay una diferencia de poder entre las personas, como ocurre entre un jefe y su empleado, o entre un paciente y su médico. Este documento establece directrices esenciales para garantizar que el tratamiento de datos personales en casos judiciales cumpla con la legalidad, idoneidad y el propósito legítimo del sistema de justicia. Por lo tanto, esta medida está en línea con la Ley Orgánica de Protección de Datos Personales (LOPDP), vinculando su aplicación directamente con los principios fundamentales del sistema judicial ecuatoriano.

2.6 Finalidad del tratamiento judicial de datos personales

El Reglamento señala que la finalidad del tratamiento de datos en juicios es principalmente salvaguardar el honor, la reputación y evitar la discriminación de las personas implicadas. A diferencia de otros contextos administrativos o de negocios, el ámbito judicial gestiona datos sumamente delicados: abarcando desde registros penales hasta datos privados relacionados con aspectos familiares, médicos, psicológicos o económicos.

En este contexto, la norma sobre el propósito específico y válido establece que el tratamiento de la información personal debe restringirse al desarrollo de tareas legales o administrativas, quedando prohibida su divulgación para propósitos diferentes que puedan menoscabar la imagen o causar estigmatización.

Principios de tratamiento aplicables en el ámbito judicial

El reglamento recoge varios principios fundamentales que orientan el tratamiento de datos dentro de los expedientes y procedimientos judiciales, tales como:

Licitud: Todo tratamiento de datos debe basarse en la ley y en las atribuciones que tenga el órgano jurisdiccional, esto significa que los jueces y funcionarios judiciales no pueden utilizar información personal fuera del marco normativo.

Consentimiento: Cuando la ley lo exija, el consentimiento del titular del dato es un requisito ineludible. Este principio cobra particular relevancia en casos que involucren menores de edad, víctimas de violencia o personas con discapacidad.

Limitación de la finalidad: Los datos no pueden ser reutilizados para fines ajenos al proceso, ni conservados de manera indefinida si su utilidad legal ha cesado.

Precisión y actualización: Los datos deben mantenerse actualizados y corregirse cuando sean inexactos. Un error en un nombre, una fecha o un antecedente puede tener consecuencias procesales irreversibles.

Seguridad: El reglamento obliga a implementar medidas de protección para evitar accesos no autorizados, pérdida de información o alteración de los expedientes judiciales, tanto en formato físico como digital (SATJE).

Responsabilidad del responsable: Establece que los responsables del tratamiento (por ejemplo, los juzgadores o los secretarios judiciales) deben garantizar que los datos se gestionen conforme al marco jurídico, así como responder por los daños derivados de su mal uso.

3. Derechos de los titulares de datos procesales

El Reglamento reconoce que las personas involucradas en un proceso judicial no pierden sus derechos como titulares de datos. Entre estos, se destacan:

Acceso: Las personas pueden solicitar el acceso a sus propios datos a través del SATJE o en la Oficina de Gestión Judicial Electrónica. Esta disposición garantiza transparencia y permite verificar el uso adecuado de los datos.

Rectificación y cancelación: Si la información consignada es errónea o desproporcionada, el titular puede pedir su corrección o eliminación, según corresponda.

Oposición: Se establece la posibilidad de oponerse a tratamientos específicos, sobre todo cuando los datos ya no son necesarios para el proceso o pueden provocar una vulneración de derechos.

4. Protección frente a la estigmatización por pasado judicial

Uno de los aportes más relevantes del Reglamento es su enfoque preventivo contra la discriminación por antecedentes judiciales. En este sentido, dispone dos garantías claves:

Ocultamiento de datos sensibles: El juzgador podrá ordenar que se oculte o reserve el acceso a ciertas providencias o documentos que contengan información sensible, cuando su exposición pueda vulnerar la intimidad, seguridad o integridad de las partes. Esto se articula con el principio de minimización de datos previsto en la LOPDP.

Tratamiento de datos en caso de sobreseimiento o inocencia: Se establece que, cuando una persona ha sido sobreseída o declarada inocente, los datos asociados a ese proceso deben ser tratados con especial cuidado, para evitar la perpetuación de una imagen negativa o errónea. Este principio reafirma la presunción de inocencia como valor constitucional y combate la "pena social residual".

5. Principio de publicidad y su limitación razonada

El sistema judicial ecuatoriano consagra el principio de publicidad como garantía de transparencia procesal. No obstante, el reglamento reconoce que este principio no es absoluto, y que debe ponderarse frente a los derechos de protección de datos personales. Esto significa que:

No toda resolución judicial debe ser publicada sin restricciones si contiene datos sensibles.

Es posible aplicar criterios de anonimización, seudonimización o restricción de acceso en casos especiales (como procesos de violencia de género, menores de edad, salud mental, etc.).

El uso de plataformas digitales no debe traducirse en la exposición masiva e irrestricta de información personal, especialmente en contextos mediáticos o con riesgo de revictimización.

Conclusiones/Recomendaciones

El análisis realizado dentro de esta investigación, generó un avance importante acerca de la prueba digital en nuestra legislación, específicamente dentro de nuestro COGEP, que es el que mas se ha podido abarcar y ha sido pauta para hacer este análisis, así como de la mano sobre la protección de los datos. Esta investigación no solo determinó la parte procesal sino también cuestiones sumamente éticas y sociales, en donde nos encontramos en una era donde nos avalancha la tecnología.

Es por ello que, a pesar de que pudimos evidenciar que en el Cogep acepta a la prueba digital como válida, existen vacíos normativos realmente preocupantes respecto a su procedimiento, a su presentación, integridad y por supuesto a su valoración, esto consecuentemente genera una desconfianza altamente jurídica, afectando de manera directa a los principios derechos de las personas, a la igualdad de en el proceso.

La carencia de protocolos, directrices y mas que eso de un marco legal transformado, así como la necesidad de una custodia digital, hace que su procedimiento sea mucho más difícil al contrario de una prueba que consta de soporte físico, creando así arbitrariedades o alteraciones injustas.

Sin embargo, se ha podido crear principios que subyacen esta carencia legal, como el principio de oportunidad que han ayudado como mecanismos de interpretación, pero aun así se puede evidenciar las deficiencias de las normas, porque no se puede asegurar la privacidad y autenticidad dentro de un proceso.

En este contexto, protección de estos datos es crucial. El manejo de toda esta información, si no se la lleva de manera adecuada y veraz, pueda generar consecuencias irreparables dentro del ámbito judicial, específicamente en la privacidad y autenticidad de todas las personas. Es por ello que, la Ley Orgánica de Protección de Datos Personales (LOPDP) y sus

normativas, como la Resolución 043-2024 del Consejo de la Judicatura, genera una aportación importante, que aun así deja vacíos normativos en la aplicación.

La investigación ha mostrado que las medidas de seguridad, la evaluación del impacto y la limitación de accesos a datos sensibles deben integrarse como parte de la cultura judicial institucional, más allá de un simple cumplimiento normativo.

De forma alineada con los objetivos particulares establecidos al comienzo de este estudio, se pudo verificar de manera detallada que existe una urgencia necesaria de crear y transformar ciertos parámetros en donde garanticen la seguridad y protección de los datos personales, sugiriendo un balance entre la publicidad del proceso y la salvaguarda de derechos fundamentales.

Para terminar, este análisis argumenta que la digitalización de la prueba no slo puede ser adoptada como una evolución más, sino que debe estar apegada a la realidad de todas las personas y que por ende esta transformación y evolución debería ser optada también dentro de un ámbito procesal y judicial, en los principios, responsabilidades y derechos de cada uno de nosotros. Tomarlo de una manera de modernizar nuestro cuerpo normativo haciendo de el algo mucho más rápido que cuente de celeridad y eficacia desde el primer momento en que nos encontramos en un proceso legal.

Así como también, una oportunidad de cambio de nuevas capacitaciones a todo el personal involucrado, como lo son jueces, fiscales, secretarios, abogados. Pero esto va de la mano de la participación presente, continua y activo del Gobierno, para que mejor la infraestructura, que se cuente con todos los implementos necesarios, para poder hacer un mejor trabajo en equipo.

Es por ello que, en esta época de la era digital, se puede garantizar de manera proactiva y eficaz los derechos de cada una de las personas, utilizándolo como un medio para potenciar en las falencias que se hayan podido determinar, y no como un riesgo de alteración.

Bibliografía

Admisibilidad de la prueba digital y su eficacia procesal según el art 202 del COGEP" Repositorio UCSG: http://repositorio.ucsg.edu.ec/bitstream/3317/23538/1/UCSG-C35-23110.pdf

Asamblea Nacional del Ecuador. (2002). Ley de Comercio Electrónico, Firmas y Mensajes de Datos. Ministerio de Telecomunicaciones. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Asamblea Nacional del Ecuador. (2008). Constitución de la República del Ecuador [Última reforma: 2021]. Registro Oficial Suplemento N.º 449. https://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

Asamblea Nacional del Ecuador. (2015). Código Orgánico General de Procesos. Ministerio de Telecomunicaciones. https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/09/Codigo-Org%C3%A1nico-General-de-Procesos.pdf

Asamblea Nacional del Ecuador. (2021). Código Orgánico Integral Penal: Actualización febrero 2021. Ministerio de Defensa Nacional. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Bulnes, M. J. (23 de mayo de 2016). La prueba digital: una realidad en el proceso civil . Obtenido de Nuevos horizontes del derecho procesal : https://books.google.es/books?hl=es&lr=&id=9ra9DwAAQBAJ&oi=fnd&pg=PA341&dq=%22prueba+digital%22+%2B%22concepto%22&ots=6r4hnwKp1K&sig=AxHNzoFPRF7cms8VIq75ppIwl2M#v=onepage&q=%22prueba%20digital%22%20%2B%22concepto%22&f=false

Consejo de la Judicatura. (2024). Reglamento para el tratamiento de datos personales dentro de procesos judiciales (Resolución 043-2024). Quito, Ecuador.

https://asobanca.org.ec/wp-content/uploads/2024/03/Resolucion-No.-043-2024-Reglamento-regula-el-tratamiento-de-los-datos-personales-que-constan-dentro-de-los-procesos-judiciales.pdf

DocuSign. (2022, diciembre 2). ¿Qué es la NOM-151 y para qué sirve? https://www.docusign.com/es-mx/blog/nom-151

E-justicia en Ecuador: inclusión de las TIC en la administración de justicia

Financial Crime Academy. (23 de Mayo de 2024). Principios de la prueba: Autenticidad, veracidad y fiabilidad. Obtenido de https://financialcrimeacademy.org/es/principios-de-la-pruebaautenticidad-veracidad-y-fiabilidad/

Gonzalez, H. M. (s.f.). Teoría general de la prueba. Obtenido de Instituto de investigaciones Juridicas : file:///C:/Users/USUARIO/Downloads/27148-24523-1-PB.pdf

Mazón, José Luis. (2016). Ensayos Críticos del COGEP. Libro 1. Pontificia Universidad Católica del Ecuador.

Mifiel. (2023, 18 de abril). ¿Qué es un mensaje de datos y por qué es importante en los contratos digitales? Blog Mifiel. https://blog.mifiel.com/mensaje-de-datos/

Parra, D. (2019). Requisitos jurídicos para la validez jurídica de la prueba digital. Obtenido de https://repository.ucatolica.edu.co/server/api/core/bitstreams/e7f59369-5db3-4891-ad74-d53dfedb8deb/content

Parra, D. (2019). Requisitos jurídicos para la validez jurídica de la prueba digital. Universidad Católica de Colombia. Disponible en: https://repository.ucatolica.edu.co/server/api/core/bitstreams/e7f59369-5db3-4891-ad74-d53dfedb8deb/content

Piedra Iglesia, W. O. (2019). ¿Cómo trata la prueba el Código Orgánico Integral Penal de Ecuador? Revista Criterio Jurídico, 19(1), 45–62. Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=6756388

Piedra Iglesias, W. O. (2023). Repositorio Constitucional. Obtenido de http://dspace.uazuay.edu.ec/handle/datos/13206

Punguil, J. (2019). Validez y eficacia de la prueba electrónica como medio probatorio en los procesos judiciales. Obtenido de http://repositorio.ucsg.edu.ec/bitstream/3317/14040/1/TUCSG-POS-MDDP-26.pdf

Quchimbo Roman, M. B. (10 de agosto de 2024). Revista Científica. Obtenido de La admisibilidad de la prueba digital en los procesos judiciales incorporados en el Código Orgánico General de Procesos.: https://doi.org/10.23857/dc.v10i3.3972

Sacoto Romo, M. C. (1 de julio de 2021). Revista de Derecho. Obtenido de E-justicia en Ecuador: inclusión de las TIC en la administración de justicia: https://doi.org/10.32719/26312484.2021.36.5

UCTunexpo. (s.f.). Principio de comunidad probatorio en el Código Orgánico General de Procesos. Recuperado de https://uctunexpo.autanabooks.com/index.php/uct/article/download/620/1163/

Vera Quezada, D. I. (05 de Septiembre de 2024). Obtenido de Admisibilidad de la prueba digital y su eficacia procesal según el art 202 del COGEP: http://repositorio.ucsg.edu.ec/bitstream/3317/23538/1/UCSG-C35-23110.pdf

World Compliance Association. (2023). Riesgos asociados al incumplimiento de la Ley Orgánica de Protección de Datos Personales y su relación con la ciberseguridad: impactos y sanciones en Ecuador. Recuperado de

https://www.worldcomplianceassociation.com/3304/articulo-riesgos-asociados-al-incumplimiento-de-la-ley-organica-de-proteccion-de-datos-personales-y-su-relacion-con-la-ciberseguridad-impactos-y-sanciones-en-ecuador.html