UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS

CARRERA DE DERECHO

INFORME FINAL DE TRABAJO DE INTEGRACIÓN CURRICULAR, MODALIDAD EN LÍNEA

TEMA:

"DERECHO AL ACCESO A LA INFORMACIÓN PERSONAL ANTE LOS PROTOCOLOS WHISTLEBLOWING: ANÁLISIS DE LA ACCIÓN DE HABEAS DATA CASO NO. 17230-2018-19732"

Trabajo de titulación previo a la obtención del título de Abogada de la República del Ecuador

LÍNEA DE INVESTIGACIÓN: Desarrollo social y del comportamiento humano.

AUTOR:

Andrea Milena Ochoa Rodríguez

DIRECTOR:

Msc. Luis Adrián Chiliquinga Cevallos

Ibarra – Ecuador 2025

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA
AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1002381356		
APELLIDOS Y NOMBRES:	Ochoa Rodríguez Andrea Milena		
DIRECCIÓN:	Ibarra-Imbabura		
EMAIL:	amochoar@utn.edu.ec		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	0983556091

DATOS DE LA OBRA	
TÍTULO:	"DERECHO AL ACCESO A LA INFORMACIÓN PERSONAL ANTE LOS PROTOCOLOS WHISTLEBLOWING: ANÁLISIS DE LA ACCIÓN DE HABEAS DATA CASO NO. 17230-2018-19732"
AUTOR:	Ochoa Rodríguez Andrea Milena
FECHA: AAAMMDD	16/09/2025
SOLO PARA TRABAJOS DE GRADO	
CARRERA/PROGRAMA:	**GRADO** ■ **POSGRADO** ☐
TITULO POR EL QUE OPTA:	Abogada

DIRECTOR:	Msc. Luis Adrián Chiliquinga Cevallos

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 16 días del mes de septiembre del 2025

EL AUTOR:

Firma: .....

Nombre: Andrea Milena Ochoa Rodríguez

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE INTERGRACIÓN CURRICULAR

Ibarra, 22 de julio de 2025

Msc. Luis Adrián Chiliquinga Cevallos

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, el mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

Msc. Luis Adrián Chiliquinga Cevallos
C.C.: 1003841812

APROBACIÓN DEL COMITÉ CALIFICADOR

El Comité Calificado del trabajo de Integración Curricular "DERECHO AL ACCESO A LA INFORMACIÓN PERSONAL ANTE LOS PROTOCOLOS WHISTLEBLOWING: ANÁLISIS DE LA ACCIÓN DE HABEAS DATA CASO NO. 17230-2018-19732" elaborado por Andrea Milena Ochoa Rodríguez, previo a la obtención del título del Abogado de la República del Ecuador, aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte:

Firmado electrónicamente por:
LUIS ADRIAN CHILIQUINGA CEVALLOS
Validar únicamente con FirmaEC

Abg. Luis Adrián Chiliquinga C. Mgs.
DIRECTOR

ALEXANDRA CRISTINA PUPIALES PROANO
Firmado digitalmente por ALEXANDRA CRISTINA PUPIALES PROANO
Fecha: 2025.07.24 13:59:59 -05'00'

Abg. Alexandra Cristina Pupiales Mgs.
ASESORA

DEDICATORIA

A Dios, principio de toda verdad y justicia, a quien debo esta culminación, pues sin su constante guía, su gracia y su presencia, el resultado habría sido imposible. En instantes de duda y agotamiento, su amor me sostuvo, infundiéndome el coraje y la fortaleza necesarios para recuperar la confianza y persistir sin cesar.

A mi madre, por ser el fundamento inquebrantable de mi existencia. Anita, querida, tu ejemplo constante de lucha, de perseverancia y de amor incondicional ha sido mi mayor aliciente para no dejarme vencer por la vida. Gracias por mostrarme, en cada acción, que no hay barrera que no se pueda superar cuando se avanza con esfuerzo y con firme determinación.

A mi esposo, mi Lucio por caminar siempre a mi lado con paciencia, comprensión y apoyo incondicional. Gracias por sostener mis manos en los momentos más difíciles, por animarme a no rendirme y por celebrar conmigo cada escalón superado. Este título también lleva tu esfuerzo y tu gran amor.

Y a mis hijos, David, Melany, Katherine ustedes representan el sentido más profundo de este esfuerzo. Cada noche de estudio, cada sacrificio, cada reto superado, lo hice pensando en ustedes que son mi mayor inspiración y la razón por la que hoy puedo decir con orgullo que lo he logrado. Espero que este paso que hoy doy les recuerde que nunca es tarde para avanzar, que el esfuerzo siempre tiene una gran recompensa y que la formación profesional es una herramienta para ser mejores personas.

AGRADECIMIENTO

A la Universidad Técnica del Norte y a cada uno de mis profesores, agradezco, en este momento de culminación, la orientación constante y la exigencia académica que moldearon mi trayectoria. Cada consulta, cada debate y cada crítica constructiva me dotaron de herramientas que trascienden lo disciplinario e infundieron en mí un sólido sentido de responsabilidad social. Los saberes adquiridos, junto al acento en la ética y la búsqueda de la justicia, se han integrado en mi identidad profesional y guiarán mis pasos en la defensa de los derechos.

Dirijo de forma muy especial mi reconocimiento al MSc. Luis Adrián Chiliquinga Cevallos, director de tesis, y a la MSc. Alexandra Cristina Pupiales Proaño, asesora de la presente investigación, por su continua orientación y respaldo a lo largo de mi formación académica. Su respaldo ha sido particularmente decisivo en esta etapa culminante, en la que su dirección constante me ha proporcionado las herramientas necesarias para la consecución de este gran objetivo.

A mis compañeros, por ofrecerme constantemente una ayuda solidaria en las horas más críticas, por cada instante padecido y cada instante compartido en cada etapa del recorrido académico, les dirijo un abrazo sincero y les auguro excelentes futuros.

RESUMEN EJECUTIVO

Los sistemas de denuncia adoptados por organizaciones mantienen la información en un nivel de confidencialidad tal que la persona denunciada ignora la identidad del informante; esta característica evita, que pueda haber represalias. No obstante, esto evidencia la complejidad en la práctica jurídica ecuatoriana, dado que, en la actualidad, no existe una normativa puntual sobre este tema. En función del caso, el análisis se dirigió a la resolución del juez, con el propósito de determinar en qué medida el habeas data logró garantizar el derecho de la persona denunciada a acceder a sus datos, a la vez que preservó la protección de la información del denunciante. Para alcanzar esta finalidad se recurrió a un diseño cualitativo, bajo el método analítico-sintético, que cotejó posturas doctrinales y jurisprudenciales, con especial atención al asunto del caso, seguido de la delimitación del marco normativo aplicable. Se realizaron entrevistas a personas con prácticas reales, pero también personales relacionadas con la temática con el fin de enriquecer el análisis desde una perspectiva empírica. Los resultados evidenciaron que sí es posible encontrar un equilibrio entre los derechos: a la información de un titular contenido en los procesos de Whistleblowing, el derecho del accionante a tener libre acceso a sus datos personales y la confidencialidad de terceros. No obstante, se concluyó que el habeas data debe entenderse y considerarse como un canal para primeramente acceder y luego proteger los datos si fuese necesario, y no como un recurso general para obtener información con fines defensivos ante una acusación.

Palabras clave: Habeas data, derecho de acceso a la información personal, protección de datos personales, Whistleblowing, confidencialidad.

ABSTRACT

The reporting systems adopted by organizations maintain information at such a level of confidentiality that the accused person is unaware of the informant's identity; this feature prevents potential retaliation. However, this highlights the complexity of legal practice in Ecuador, since there is currently no specific regulation on this matter. Based on the case in question, the analysis focused on the judge's decision in order to determine to what extent the habeas data mechanism was able to guarantee the accused person's right to access their data while also preserving the protection of the informant's information. To achieve this, a qualitative design was used, under the analytical-synthetic method, comparing doctrinal and jurisprudential positions, with special attention to the case at hand, followed by the delimitation of the applicable regulatory framework. Interviews were conducted with individuals who have both real and personal experience related to the topic, in order to enrich the analysis from an empirical perspective. The results showed that it is indeed possible to find a balance between rights: the data subject's right to access information contained in Whistleblowing processes, the plaintiff's right to freely access their personal data, and the confidentiality of third parties. However, it was concluded that habeas data should be understood and considered primarily as a channel for accessing and, if necessary, protecting data not as a general mechanism to obtain information for defensive purposes in response to an accusation.

Keywords: Habeas data, right of access to personal information, personal data protection, Whistleblowing, confidentiality.

LISTA DE SIGLAS

CADH. Convención Americana de derechos humanos.

CNR. Consejo Noruego para Refugiados.

DUDH. Declaración Universal de Derechos Humanos.

GDPR. Reglamento General de Protección de Datos.

LOPDP. Ley Orgánica de Protección de Datos Personales.

OCDE. Consejo de la Organización de Cooperación y Desarrollo Económicos.

OEA. Organización de los Estados Americanos.

ONG. Organización no gubernamental.

ONU. Organización de las Naciones Unidas.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La Constitución de Ecuador, complementada por la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional y la Ley Orgánica de Protección de Datos Personales establece un sólido marco jurídico cuya finalidad primordial es garantizar el derecho de toda persona a acceder, examinar y proteger los datos personales en sentido estricto, además con las decisivas directrices de la Corte Constitucional, en sus Sentencias 182-15-SEP-CC y 47-19-JD/22 distinguió la protección en un sentido amplio, proveyendo a la acción de habeas data como una vía adecuada para la defensa de estos derechos.

En este sentido, el habeas data es un medio legal que ha sido consolidado como una estrategia para garantizar la privacidad, especialmente sobre el control y decisión relativa a la información personal, este derecho está intrínsecamente vinculado a la dignidad humana que además, cobra especial importancia en los protocolos de denuncia interna dentro de cada institución correspondiente o también conocidos como protocolos Whistleblowing, donde existe la manipulación de diversos datos personales y en los que los sistemas o modelos Whistleblowing por un lado están diseñados para facilitar la denuncia de conductas ilícitas o irregulares, priorizando la confidencialidad del denunciante, lo que suele condicionar el acceso del denunciado a los datos personales relacionados con él.

Este estudio se orienta y centra su análisis en el caso No. 17230-2018-19732, como un gran ejemplo de la disputa en torno al derecho de consultar datos personales y el deber de preservar la confidencialidad en los protocolos de denuncia interna en organizaciones internacionales establecidas en Ecuador, en esta indagación investigativa el objeto de estudio es la aplicación de la acción de habeas data como garantía jurisdiccional que busca equilibrar los derechos en juego: el del denunciante a mantener sus datos en anonimato y el del denunciado a conocer los datos

personales o información que se le relaciona y obra en su contra, este caso resulta relevante al evidenciar cómo los jueces pueden ponderar derechos en contradicción, proponiendo soluciones que fortalecen tanto la transparencia como la protección de la intimidad, especialmente dentro del marco de los protocolos Whistleblowing.

Formulación del problema

La acción de habeas data como mecanismo de salvaguarda, junto con el ejercicio del derecho de acceso a información personal en el contexto de los protocolos de prevención de delitos internos, plantea un gran conjunto de problemas tanto jurídicos como éticos. La complejidad se deriva, principalmente, de la exigencia de equiparar de forma adecuada la defensa de dos derechos que, aparentemente, pueden entrar en conflicto, tal como la intimidad o privacidad y el deber de asegurar la transparencia en la gestión de los informes internos dentro de las organizaciones. Los protocolos de Whistleblowing a menudo garantizan la confidencialidad del denunciante para fomentar la denuncia de conductas ilícitas, sin embargo, esto puede bloquear el acceso del denunciado a la información recopilada en relación a él y con respecto en su contra (Garrido, 2024).

Además, la digitalización y el uso de sistemas automatizados para la gestión de denuncias introducen algunos riesgos adicionales relacionados con la seguridad y la privacidad de la información, por otra parte, los denunciados tienen derecho a conocer y rectificar la información personal contenida en las denuncias para que les permita tener un proceso justo y equitativo, este derecho entra en tensión directa con la obligación de preservar el anonimato del denunciante, generando un conflicto constitucional entre dos principios: el derecho a la defensa y el derecho a la protección de datos personales (Cruz, 2023).

La falta de un adecuado balance puede ocasionar la trasgresión de los derechos de privacidad del denunciante o del derecho al acceso a la información del denunciado, así mismo, una gestión inadecuada de los protocolos de Whistleblowing puede generar desconfianza tanto en los denunciantes como en los denunciados, afectando la transparencia y la ética organizacional, en este sentido, las organizaciones pueden enfrentar sanciones legales por no cumplir con la normativa que dirige el resguardo de datos, así también responder a litigios por vulneraciones de derechos individuales. Una sensación de injusticia o falta de protección puede deteriorar la cultura organizacional, desincentivando la denuncia de conductas indebidas y perpetuando prácticas ilícitas.

Planteamiento de los objetivos

Objetivo general

Analizar la acción de habeas data como mecanismo de protección del derecho de acceso a la información personal en el marco de los protocolos de denuncia interna Whistleblowing, a través del estudio del caso No. 17230-2018-19732.

Objetivos específicos

- Examinar criterios teóricos, normativos y jurisprudenciales del derecho al acceso a la información personal y su relación con la protección de datos personales.
- Describir los efectos generados de la activación acción de habeas data caso No. 17230-2018-19732 sobre el derecho al acceso a la información personal, en el contexto de los protocolos de denuncia interna Whistleblowing.
- Determinar la idoneidad del derecho al acceso a la información personal en el contexto de los protocolos Whistleblowing, a través del estudio del caso No. 17230-2018-19732.

Pregunta de investigación

¿De qué manera la acción de habeas data garantiza el derecho de acceso a la información personal sin vulnerar el derecho a la protección de datos personales del denunciante en el contexto de los protocolos de denuncia interna Whistleblowing, según lo demuestra el análisis del caso No 17230-2018-19732?

Justificación

El derecho a acceder a la información personal es una potestad básica que permite a cada persona conocer qué datos le conciernen que posee un tercero, con qué propósitos son tratados y si son exactos. En Ecuador, tal derecho es un pilar del régimen de protección de datos, circunstancia que la Corte Constitucional ha corroborado reiteradamente al calificarlo, a la vez, como un elemento del habeas data. De la misma forma, la Ley Orgánica de Protección de Datos Personales (2021) no se limita a reconocer el acceso como una garantía que asiste al titular para recibir sus datos, sino que articula, además, mecanismos complementarios orientados a su salvaguarda.

Hoy en día, proteger los datos personales es una de las prioridades más importantes, tanto en el derecho como en la tecnología. Cuando una denuncia se tramita a través de los canales internos de una institución, la acción de habeas data juega un papel sumamente importante. Esta acción judicial permite que la persona acceda a su información sin poner en riesgo la confidencialidad de los datos de otros. Esto pone de manifiesto que el asunto es serio: hay que diseñar normas que regulen cómo se pueden usar los datos personales en estos procesos internos. Así, se evitan violaciones de derechos y se asegura que todas las partes sean tratadas de manera justa.

En esta investigación se analiza el rol de la acción de habeas data como garantía jurisdiccional, en la protección del derecho de acceso a la información personal dentro de los protocolos de Whistleblowing, a través del estudio del caso N° 17230-2018-19732 (2019), en el que el conflicto de derechos que se aborda es la tensión entre la necesidad de cuidar y proteger la identidad y confidencialidad de los denunciantes (whistleblowers) en investigaciones internas por presuntas infracciones, y el derecho del denunciado a acceder a sus datos e información personal vinculados a la acusación, incluyendo "tiempo, lugar y modo" de los hechos, e incluso la identidad de sus acusadores, este dilema se centra en determinar hasta qué punto la privacidad del denunciante prevalece sobre el derecho del acusado a la información, la defensa y la protección de su intimidad, dignidad y bienestar emocional, que pueden verse afectados por una denuncia.

El caso en cuestión fue resuelto por la Dra. Carmen Romero Ramírez jueza de la Unidad Judicial Civil del Distrito Metropolitano de Quito, quien encontró un balance entre los derechos en conflicto, inclinándose parcialmente a favor del denunciado, además enfatizó la igualdad procesal de las partes y aunque concedió el acceso a la información relevante sobre los hechos, protegió la identidad del denunciante al excluir cualquier dato que pudiera revelar quién era.

En este contexto, lo que se pretende es generar conocimiento sobre cómo la aplicación de esta garantía jurisdiccional promueve de manera efectiva el equilibrio de los derechos del denunciante y del denunciado en referencia a la información, acceso y correspondiente cuidado de datos, finalmente se busca la comprensión de los principios aplicados en el caso específico.

El estudio además de implicaciones teóricas ofrece beneficios para la práctica jurídica, la academia y la sociedad en general. Desde la mirada del derecho, este trabajo entrega pautas concretas que pueden usar jueces, abogados y legisladores para perfeccionar la denuncia protegida, o Whistleblowing, asegurando que cada acción se funde en criterios claros y razonados. A nivel

académico, enriquece la bibliografía de la materia, sirviendo como base para la investigación futura en derechos conexos, como la protección de datos personales. Por último, en la esfera social, la investigación despierta una mayor sensibilización sobre el peso jurídico que tiene el derecho individual a los datos y la urgente necesidad de gestionarlos de modo seguro y transparente dentro de las organizaciones.

CAPÍTULO I: MARCO TEÓRICO

1.1. La protección de datos personales, tensión entre derechos (privacidad y acceso)

En Ecuador se presentan organismos internacionales que ejecutan protocolos internos basados en normativas y estándares foráneos, lo cual responde a la propia naturaleza transnacional de estas entidades. Esta tendencia, aunque busca fortalecer mecanismos de denuncia e investigación como el Whistleblowing, ha suscitado preocupaciones en torno al equilibrio entre la protección del denunciante y las garantías del denunciado, en este sentido Ballesteros (2020) advierte sobre la tendencia hacia una protección excesiva del denunciante, lo que puede limitar los derechos del denunciado, su estudio aboga por estrategias como la anonimización y el acceso controlado a material informativo, proponiendo soluciones que permitan armonizar la protección de la identidad de un denunciante con los derechos del denunciado.

En este aspecto, la protección de datos constituye el conjunto de normas, principios y mecanismos técnico jurídicos diseñados de manera específica para salvaguardar la privacidad en el ámbito del tratamiento de la información personal, asegurando de esta forma el control del individuo sobre cómo sus datos son recopilados, usados y almacenados por terceros (Chipuxi & Guaña, 2023). Es esencial aclarar que para que exista protección de datos personales debe garantizarse la privacidad, esto se refiere a que su titular mantenga su esfera íntima privada de intrusiones ajenas sin su consentimiento, controlando el flujo de información sobre sí misma.

En el Ecuador se garantiza el derecho a la protección de datos personales mediante la Constitución (2008), que en su Art. 66 numeral 19 menciona:

El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión

sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

Es así que la protección de datos personales es un derecho que permite la privacidad y seguridad de la información, su desarrollo inició a finales del siglo XIX con la idea del derecho a "ser dejado en paz" (Pérez, 2019, p. 3), en relación a la libertad y privacidad, fue reforzado por la Declaración Universal de los Derechos Humanos en los artículos 12 y 19, además de la Convención Americana de Derechos Humanos en sus artículos 11 y 13, estos instrumentos permiten el acceso a la información y protección de los datos personales (Maqueo et al., 2017).

En respuesta a la creciente preocupación por el uso de datos personales, países como Alemania y Suecia lideraron la promulgación de leyes específicas, como la Convención 108 del Consejo de Europa en 1981 y la Directiva de la Unión Europea en 1995, en los cuales se establecieron altos estándares de protección (Bru, 2007). Posteriormente se desarrolló, el Reglamento General de Protección de Datos de 2018, que otorgó a los ciudadanos derechos, como el derecho al olvido y la portabilidad de datos (Zaror, 2019).

La proliferación de tecnologías avanzadas particularmente la inteligencia artificial y el análisis masivo de datos, ha hecho que la protección de datos sea más compleja y prioritaria, debido al incremento y uso masivo de datos a nivel mundial. En América Latina, en países como Argentina y Brasil en 1994 en 1988 correspondientemente, incorporaron el habeas data en sus constituciones y adoptaron leyes inspiradas en marcos internacionales, como las directrices emanadas por el Consejo de la Organización de Cooperación y Desarrollo Económicos (OCDE) de Europa (Bazán, 2005; Bru, 2007). Lo que impulsó la adaptación de normativas como la Ley de Privacidad del

Consumidor de California del 2020 y la promulgación de la Ley Orgánica de Protección de Datos Personales en Ecuador (LOPDP) en el año 2021 (Barrio, 2022; Rovira et al., 2023).

La LOPDP (2021) tiene como propósito asegurar el cuidado de los datos personales, garantizando el derecho de acceso, control y seguridad sobre dicha información mediante la aplicación de principios previamente establecidos en la resolución 45/95 de la ONU y el Comité Jurídico Interamericano de la OEA en 2021. De esta forma, la privacidad y seguridad ha pasado de ser una preocupación teórica para convertirse en una prioridad legal y política a nivel global, en un contexto donde la información concerniente a una persona es un recurso sumamente valioso, el mismo que a falta de una protección adecuada puede ser vulnerado.

1.1.1. Derecho al acceso a la información personal

El derecho de acceso a la información es el que permite a las personas tener la libertad de investigar sobre un colectivo general de datos, sin embargo, su acceso se limita principalmente a los datos propios del titular y no a un acceso libre de cualquier dato que puede afectar a terceros, esta capacidad dota al individuo de un poder, el mismo que se exterioriza en su derecho a su autonomía y su libertad de expresión sobre la información accedida (Carbonell, 2006). Es pertinente distinguir entre los diferentes tipos de datos, ya que algunos son de carácter público, mientras que otros son de naturaleza personal y, por lo tanto, requieren una protección especial.

En el Ecuador la Constitución (2008), específicamente en el artículo 66 en la sección que corresponde a los derechos de libertad, numeral 19, establece el derecho a acceder a datos de carácter personal, además que faculta a su titular tomar una decisión sobre la misma con la finalidad de protegerla. Este derecho al estar relacionado con la protección de datos contiene elementos importantes que permiten conocer sobre la información que se recopila, cómo se utiliza, y con qué fines, elementos esenciales para la custodia de datos en general (Quiroz, 2016).

La Ley Orgánica de Protección de Datos Personales (2021) es la normativa principal que regula el tratamiento de datos personales en Ecuador, en su artículo 13 establece el derecho a acceder y menciona la obligatoriedad a responder a solicitudes de acceso en un plazo razonable de quince días, esta ley se encuentra al nivel de los criterios internacionales como el GDPR de la Unión Europea, es decir que las organizaciones están legalmente obligadas a responder a las solicitudes de acceso, este derecho asegura que los datos no sean empleados para propósitos diferentes a los inicialmente indicados sin obtener el consentimiento explícito del titular (Bernal-Camargo & Gómez-Córdoba, 2022), de esta manera facilita que las personas puedan mantener el control sobre su información y garantizar que esta se utilice de manera compatible con las expectativas y permisos, esto contribuye a la protección adecuada y el tratamiento justo de la información personal.

Una vez que el individuo haya accedido y comprendido de forma completa las circunstancias en que se encuentra su información personal, y con el fin de ejecutar de manera efectiva la protección de datos, el interesado puede aplicar según las necesidades identificadas, el principio de autodeterminación informativa, el mismo que representa una concreción del derecho a la protección de datos personales, en consecuencia, el derecho de acceso a la información personal no actúa de forma aislada, sino que más bien se integra dentro de un conjunto más amplio de derechos orientados a que se establezca la autonomía de los individuos sobre sus datos.

1.1.2. Derecho de confidencialidad y protección de la privacidad

Existe un vínculo estrecho entre la acción de habeas data y la confidencialidad debido a que éstos son mecanismos que ayudan a garantizar que la información se mantenga en secreto y solo sea accesible para personas autorizadas (Ormazabal, 2021). La confidencialidad facilita la protección de la privacidad y es fundamental que se establezca en las legislaciones de protección

de datos (Quiroz, 2016), de esta manera los datos personales pueden ser tratados de manera confiable, segura y protegidos contra el acceso no autorizado o la divulgación indebida de parte de terceras personas. Cuando la confidencialidad se muestra afectada, el habeas data es el mecanismo procesal que permitirá al individuo actuar de forma rápida y oportuna para restaurarla, sea que estuviera vulnerada o en riesgo.

El Ecuador, como estado miembro de la OEA, refuerza su compromiso con la protección de la privacidad, es así que en la Constitución (2008) se establece el principio de confidencialidad para salvaguardar el derecho a la privacidad y protección de los datos e información de las personas en el artículo 66, numeral 19, 20 y en concordancia, con el artículo 40, numeral 5 que establece la obligación del Estado para proteger la información personal de todos los ciudadanos, garantizando la confidencialidad incluso cuando los datos se encuentren en registros de instituciones nacionales fuera del territorio ecuatoriano, de la misma forma, tal como lo establece la Ley Orgánica de Protección de Datos Personales (2021) en su artículo 10 literal g) y j) que implica que la información debe ser tratada de manera reservada contra intrusiones no autorizadas.

Para que la mencionada normativa se cumpla y se aplique de forma adecuada se ha creado como ente rector a la Superintendencia de Protección de Datos Personales del Ecuador, la misma que para la aplicación efectiva del principio de confidencialidad y otros, recae directamente sobre el Superintendente que es la autoridad competente en esta materia. Este órgano de control no solo supervisa y evalúa las actividades de quienes tratan datos personales, sino que también posee una potestad sancionadora para corregir y sancionar incumplimientos a este deber de reserva, esto se lo realiza a través de la resolución de reclamos, la realización de auditorías y la emisión directrices técnicas, de esta manera se garantiza que los datos se mantengan resguardados y se prevenga su acceso o divulgación no autorizada (Ley Orgánica de Protección de Datos Personales, 2021).

En este aspecto, las organizaciones tienen una gran responsabilidad que es implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, protegiéndolos contra el acceso no autorizado, especialmente cuando exista la posibilidad de la divulgación accidental o ilegal (Lisoni, 2020). Solo las personas autorizadas, que necesitan acceder a los datos personales para cumplir con sus funciones específicas, deben tener acceso a esta información, para lograr esto, se deben aplicar prácticas como la verificación de identidad de los usuarios, la codificación de datos y la monitorización de accesos, con el fin de prevenir el uso no autorizado y asegurar una gestión adecuada de la información.

Otro factor importante es que las organizaciones deben obtener el consentimiento informado, que según Buedo et al. (2023) se refiere a la autorización que una persona da para el uso de su información personal, el cual debe presentarse antes de recolectar y procesar su información identificativa, además de limitarse a fines específicos y legítimos, no se debe tratar la información de manera incompatible con estos fines originales, es así como, la minimización de datos es un aspecto crucial, por lo que las organizaciones deben restringir la recolección de datos a lo estrictamente necesario, evitando recopilar más información de la que realmente se requiere para el tratamiento previsto (Chana, 2022).

A nivel internacional, el respeto por la confidencialidad se empezó a ver con claridad gracias al Comité Jurídico Interamericano de la OEA. Este Comité dice que la información personal de cada persona solo debe quedar protegida y no se puede contar o revelar a otros que no tengan un motivo justo (OEA, 2022). Además, este principio coincide con otros acuerdos y normas internacionales, como el Reglamento General de Protección de Datos de la Unión Europea y la Convención 108 del Consejo de Europa, lo que resalta que el respeto a la confidencialidad es fundamental para salvaguardar la privacidad de las personas. Esta normativa internacional a

excepción de la establecida por la OEA no influye de forma directa debido a que, más bien ha servido de base o modelo para la creación de una normativa propia ecuatoriana adaptada a estos estándares internacionales (García, 2024).

Por otro lado, (Andía & Colombato, 2021) comentan que existe conflicto en la protección de la privacidad de los datos de diversas personas dentro de un registro, especialmente cuando estos incluyen información tanto pública como privada, por tal razón, el principio de proporcionalidad del tratamiento de datos exige que solo se recojan y utilicen aquellos datos que sean estrictamente necesarios y pertinentes para el fin perseguido (Laro, 2021), además es fundamental realizar una distinción adecuada de los datos personales y aplicar el principio de disociación, esto asegura que la información difundida sea tratada de manera que no pueda vincularse ni asociarse al titular, preservando su privacidad y garantizando que su identidad permanezca protegida e inidentificable (Ticli, 2021).

En consecuencia, al aplicar estos principios, se puede establecer que la información personal del titular se reduzca en la cantidad y exclusividad del tipo de información, además la disociación coadyuva a no asociar ni identificar de manera inapropiada a una persona, de esta manera se revela una articulación en torno al principio de confidencialidad y protección de la privacidad en el manejo de datos concernientes a una persona, mismas que se complementan con los principios de disociación y proporcionalidad del tratamiento.

1.2. Habeas data en la Constitución ecuatoriana

1.2.1 Origen y evolución

Desde el punto de vista Etimológico, el habeas data proviene de la palabra “habeo” que tiene relación en su significado con el término “posesión”; el término “data” que refiere a “datum”, que alude a lo que se da o dato, este se refiere a datos contenidos en hechos, conceptos y protocolos

y que a su vez sirven como medio de comunicación y entrega (Mora, 2019). Es decir, se relaciona con la noción de posesión y entrega de datos, ha desarrollado su significado hasta consolidarse como un derecho que permite a cada individuo que obtenga y administre lo concerniente a su información personal.

En Ecuador, el habeas data fue introducido inicialmente en la Constitución de 1996, como parte de las garantías de los derechos, y definía el derecho de toda persona a consultar la información vinculada a ella o sus bienes que constara en órganos de carácter estatal o particular, así como a informarse sobre el uso de esos datos y su finalidad. También permitía solicitar el ajuste o anulación de la información si era equívoca o afectaba ilegítimamente sus derechos, con excepción de datos reservados por motivos de seguridad nacional.

En 1997, la Ley de Control Constitucional incluyó un marco normativo específico permitiendo a las personas naturales o jurídicas, nacionales o extranjeras, acceder a la información, de la misma forma como se estableció en la actual Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), pero con una notable variación que refleja su evolución al ampliar, consolidar y modernizar dicho marco procesal, de esta manera se unificó el sistema de garantías jurisdiccionales bajo una misma normativa. Así mismo, en la Constitución de 1998, se adicionó la capacidad de demandar indemnización si la falta de respuesta causaba perjuicio.

Finalmente, en la Constitución (2008) se amplió y consolidó esta garantía, misma que en su artículo 92 se detalla "…derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, (…) en soporte material o electrónico. Asimismo tendrá derecho a conocer (…) el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.", es decir que de forma relevante se incluyó el acceso a datos o documentos estructurados digitalmente y el

reconocimiento del derecho a conocer la duración de su almacenamiento (Gárate et al., 2021). Estas consideraciones conllevan hacia una protección constitucional más integral y efectiva considerando las tendencias tecnológicas de la actualidad.

La evolución de esta garantía y las reformas constitucionales del Ecuador ha sido relevantes en el fortalecimiento del acceso y la protección de los datos personales, que van desde su introducción, hasta su reafirmación y posterior consolidación en la actual Constitución (2008), donde se ampliaron los derechos y se consolida con un enfoque integral en la protección de la privacidad de los ciudadanos, al ampliar su alcance se adapta al entorno tecnológico que ha sido crucial frente a las dinámicas digitales contemporáneas, esto debido a que la protección de datos personales se ha vuelto más compleja y crítica (Pérez, 2023). La evolución de este marco normativo refleja la creciente importancia del habeas data y la continua adaptación de las normativas para precautelar los derechos de las personas con respecto a sus datos en la era tecnológica.

1.2.2. Aplicación del habeas data

En la actualidad, el habeas data se establece como una garantía jurisdiccional que ayuda a las personas a acceder de forma judicial a sus datos y, a partir de dicho acceso, decidir que curso toma o aplicar una acción más adecuada para proteger su información (Alzate et al., 2024), esta garantía se proyecta como una herramienta esencial para la defensa de derechos lesionados relacionados con la privacidad y la integridad de los datos personales, garantizando que estos no sean utilizados de forma indebida o sin el consentimiento de su titular, manteniendo un control sobre la información y para que las entidades manejen la información con la debida confidencialidad y seguridad (Garcés et al., 2023; Garrido, 2024). De esta manera se obliga al

respeto de los derechos establecidos en la Constitución y la Ley Orgánica de Protección de Datos Personales.

El habeas data también figura en instrumentos internacionales que garantizan la protección de datos personales mediante el principio de autodeterminación informativa que para Bonilla (2024) es la capacidad de las personas para gestionar de forma integral sus datos para su protección. Por su parte, la jurisprudencia ecuatoriana ha abordado y desarrollado el concepto de autodeterminación informativa en varias sentencias, consolidando su entendimiento como un poder fundamental del individuo sobre sus datos personales, un ejemplo es la sentencia No. 2064-14-EP/21, en la cual se entiende como el autocontrol y la autonomía de decisión que aborda el individuo respecto a su propia información personal.

En este contexto, se puede entender que este principio está integrado por otros subprincipios establecidos tanto por la Asamblea General de la ONU (1990), como por el Comité Jurídico Interamericano de la OEA (2022) y relacionado con el artículo 11 de la Convención Americana sobre Derechos Humanos OEA (1969), es decir que el habeas data no figura únicamente como una garantía, sino también como un derecho fundamental que está intrínsecamente vinculado, en esencia, a los derechos de libertad y dignidad.

En la normativa internacional, la DHDH, en el artículo 12, ha establecido la negativa de "injerencias arbitrarias en su vida privada" (Naciones Unidas, 1948, p. 4). En el mismo contexto lo establece el PIDCP de 1966 en su art. 17, pero adiciona en su numeral 2. "la protección de la ley contra esas injerencias" (Naciones Unidas, 1966, p. 7). En este sentido, lo expuesto ha sentado las bases para la elaboración de un marco normativo en Ecuador, destinado a garantizar el acceso, conocimiento y protección de los datos personales, vinculados directamente con la privacidad.

La Corte Constitucional ha dejado claro, aunque no siempre de manera directa, que todos los derechos son para todos, especialmente cuando se trata de que nadie puede intervenir de manera arbitraria en la vida privada de las personas. También ha subrayado que todos cuentan con protección legal frente a esos abusos. Al estudiar el habeas data y el derecho a controlar la propia información, ha utilizado el bloque de constitucionalidad, que permite que los tratados internacionales de derechos humanos se apliquen en Ecuador como si fueran parte de la Constitución misma. De esta forma, la Corte ha argumentado que el derecho a la protección y autodeterminación son extensiones necesarias de la garantía a la vida privada, asegurando que el individuo mantenga el control sobre sus datos y su dignidad, conforme a los estándares internacionales (Sentencia 001-14-PJO-CC, 2014).

Por otro lado, El habeas data se encuentra en la necesidad de que se busquen vías o se adapten los derechos tradicionales de privacidad a las realidades de la era digital, donde la información personal puede ser fácilmente recolectada, almacenada y posiblemente difundida.

Actualmente, en el Ecuador esta garantía está consagrada en la Constitución (2008) en el artículo 92 que reconoce el derecho de toda persona a acceder a sus datos personales, mientras que la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009) es la norma que establece la regulación de las garantías jurisdiccionales constitucionales, esta ley a través del artículo 49 al 51 permite la aplicación específica del habeas data, además para el desarrollo de la misma, la Corte emitió un dictamen para evitar su desnaturalización y en su Sentencia 182-15-SEP-CC (2015) ha establecido reglas jurisprudenciales como: naturaleza, contenido y alcance de la acción con efectos erga omnes, de modo que se traduce en la creación de un precedente de vinculación y obligatoriedad para una totalidad de individuos, entidades y autoridades (Ayala et

al., 2024). Estas reglas van encaminadas a la protección de la intimidad, el honor y la integridad psicológica de las personas, evitando la divulgación no autorizada de información.

Este marco legal garantiza el derecho de acceso a la información personal como una acción jurisdiccional, asegurando que las entidades encargadas de recopilar y manipular los datos personales actúen con responsabilidad, transparencia y respeto frente a las solicitudes de acceso de los individuos en referencia a sus datos personales, con el fin de proteger de manera eficaz y rápida los derechos que les corresponden.

1.2.3. Principales componentes o principios del habeas data en el Ecuador

El derecho o facultad de rectificación, actualización y cancelación de datos personales son componentes esenciales del habeas data, como un derecho en las legislaciones de protección y cuidado de datos en todo el mundo (Porcelli, 2019), esta garantía está estructurada por estos aspectos que permiten la protección de datos de forma integral, Garrido (2024) también considera al acceso o la obtención de información como principal componente, seguido de la confidencialidad que es fundamental para la protección, este último componente da la garantía para que los datos personales serán tratados con privacidad y seguridad. La integración de estos derechos faculta a los individuos para mantener controlados los aspectos sobre su información.

La noción de la palabra “componentes” del habeas data en el derecho ecuatoriano no se refleja expresamente en la normativa, más bien ha sido una construcción doctrinaria basada en las necesidades, principios y elementos normativos que estructuran la aplicación del habeas data para el efectivo ejercicio de los derechos, en esta línea de ideas, lo ha desarrollado la jurisprudencia de la Corte Constitucional de forma análoga a la doctrina como: “…dimensiones utilitarias de esta garantía acorde al objeto específico que puede perseguir…”(Sentencia 182-15-SEP-CC, 2015), dentro de las cuales están: la dimensión informativa y de reserva, especialmente relevante en casos

de Whistleblowing donde se requiere aplicar las dos dimensiones para ejercer los derechos de las partes involucradas. Finalmente, el habeas data cancelatorio permite al titular solicitar la eliminación de datos sensibles o innecesarios (Espinosa, 2017), el mismo que se alinea con el principio de minimización de datos, promovido por normativas nacionales e internacionales para evitar la recopilación y conservación excesiva de información personal.

Los componentes informativo y reserva del habeas data resultan especialmente pertinentes para los titulares, no obstante, esta reserva no puede ser absoluta ni utilizarse como barrera para negar el acceso a información sustancial y correspondiente ejercicio de sus derechos. Por tanto, ambos aspectos del habeas data deben ser aplicados de forma armónica, permitiendo salvaguardar la integridad del denunciante sin menoscabar el derecho del denunciado a acceder a la información que lo concierne y que resulta indispensable.

En definitiva, el derecho de acceso como principal elemento, tal como lo menciona Garrido es un derecho que se articula con los demás componentes del habeas data para conseguir su finalidad protectora, estos elementos además guardan concordancia con el tercer párrafo del artículo 92 de la Constitución del Ecuador y se relacionan con los artículos 13, 14 y 15 de la Ley Orgánica de Protección de Datos Personales (2021) que dispone el reconocimiento de estos componentes como derechos, según lo previsto en la Constitución, con la finalidad de que los titulares de datos conozcan sobre la gestión de sus datos y tengan acceso gratuito a los mismos.

1.2.4. Requisitos para la activación del habeas data

El habeas data se enmarca exclusivamente a datos o información estrictamente de carácter personal, por lo tanto, el dato personal es una característica fundamental contenida dentro de los requisitos para su activación en el ámbito de protección de datos, bajo esta perspectiva, es necesario aclarar que los datos personales son cualquier tipo de información o detalle que se

relacione con una persona física y que los mismos permitan identificarla o que pueda ser individualizada de manera directa o indirecta, tal y como puede ser a través de un número de identificación o características particulares de su identidad física, social o económica, es así que una persona puede ser identificada, cuando la información permite su reconocimiento sin requerir medios adicionales para determinar su identidad (Polo, 2020, p. 180).

En este contexto, la idea se encuadra en lo que establece la Ley Orgánica de Protección de Datos Personales (2021), específicamente en su artículo 4 en el que se establece que los datos personales son los que permitan identificar de manera explícita o implícita a la persona, de la misma forma como puede identificarse mediante características particulares de su identidad, de conformidad con lo expuesto por la Corte Constitucional en la Sentencia: No. 47-19-JD/22 (2022) en donde aclara que para considerase un dato como personal deben contener elementos que funcionan como "identificadores" los mismos que permiten determinar la singularidad de una persona, además, menciona que corresponden a datos de su titular los detalles sobre las relaciones de él con terceros y que los aspectos de su entorno laboral o familiar pueden hacer que sea identificable, ya sea de manera directa o también indirectamente, en consecuencia, este tipo de información es susceptible de ser solicitada por medio habeas data, quedando en manos de los jueces la evaluación de su relevancia en atención a las particularidades de cada caso.

La admisión y activación del habeas data depende de la configuración de los requisitos dispuestos en el artículo 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009) que establece principalmente tres aspectos, los cuales deben definirse al momento de que el titular solicite formalmente su información al tenedor de los datos, estos son: la existencia de una negativa tanto a conceder el acceso directo, como la negativa a la solicitud de realización de algún cambio en los datos erróneos, por parte sea de una entidad pública o persona

natural o jurídica del sector privado, o cuando se proporcione un mal uso de los datos personales que puedan afectar los derechos constitucionales de un individuo, los cuales pueden ser los derechos establecidos en los numerales 19 y 20 del artículo 66 de la Constitución (2008).

En este aspecto, cabe precisar también que un factor relevante para que se pueda interponer la acción de habeas data según la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009) establecida en el Art. 51 es la legitimación activa que recae en el titular de los datos o información, sea esta persona natural o jurídica, mientras que la legitimación pasiva corresponde a cualquier tipo de entidad o persona que contenga la información sea en el ámbito público como privado (Constitución, 2008).

La Corte Constitucional también ha desarrollado la legitimación de las partes procesales en la acción de habeas data, pero de forma implícita, es así que en la Sentencia 182-15-SEP-CC (2015) se detalla la naturaleza de la acción donde el legitimado activo debe proponer la garantía considerando todos los parámetros establecidos en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (2009), esta consideración es relevante porque la Corte profundiza en la naturaleza de la acción y al hacerlo, se refiere a quién puede ejercerlo y contra quién, reforzando la idea de que es el titular de los datos quien tiene la facultad de acción sobre el tenedor de los datos, que bien pueden ser parte del Estado o particulares, además con igual consideración ha enfatizado que el habeas data no se limita únicamente a garantizar el acceso, sino que también comprende facultades esenciales como la rectificación, actualización y supresión de los datos cuando sea exista la necesidad o vulneren derechos (Sentencia No. 2064-14-EP/21, 2021).

1.3. Protocolos Whistleblowing

Los protocolos de Whistleblowing, también son conocidos como sistemas de denuncia o canales de reporte ético en las instituciones, estos son mecanismos establecidos por entidades que

facilitan a los empleados y partes interesadas la posibilidad de reportar de manera segura y confidencial irregularidades como conductas indebidas, fraudes, abusos, o cualquier otra actividad contraria a las normativas internas o externas de la organización (Sánchez, 2010), así que estos protocolos facilitan la detección temprana de malas prácticas, promueven una cultura de integridad y responsabilidad de los trabajadores dentro de las entidades.

En otras palabras, los protocolos Whistleblowing son sistemas sistemáticos, estructurados y formales que permiten a los individuos dentro de una organización reportar de manera confidencial y segura cualquier tipo de preocupación relacionada con conductas inapropiadas o ilegales que afecten a dicha organización (Echeverría, 2013), por lo tanto estos sistemas están diseñados para proteger a los whistleblowers (denunciantes) de repercusiones y garantizar que sus denuncias sean investigadas de manera adecuada y sin prejuicios.

Una cualidad que destaca principalmente en este tipo de denuncias es la preservación de la confidencialidad de los denunciantes, con el objetivo de prevenir represalias por parte de los denunciados. Por esta razón, la gestión de la información contenida en los expedientes investigativos que lleva de forma interna una institución incluye tanto los datos del denunciante como del denunciado, así como informes y los detalles de los actos o hechos denunciados, toda la información tratada mediante estos protocolos debe ser estrictamente reservada.

En el Ecuador actualmente no existe una norma o ley que regule de forma directa los mecanismos de denuncias internas bajo la modalidad Whistleblowing en instituciones del sector privado y público, esta mención es respaldada por la Corte Interamericana de Derechos Humanos que en el caso Julio Rogelio Viteri Ungaretti vs. Ecuador que mencionó:

> "…la ausencia de mecanismos de denuncia adecuados y la ausencia de mecanismos de protección de denunciantes de actos de corrupción constituye una violación a la obligación

de adoptar disposiciones de derecho interno para hacer efectivo el derecho a la libertad de expresión…".(Castillo, 2024)

Si embargo, ante este panorama surge el papel o rol de la Contraloría General del Estado que es fundamental en el control tanto de uso de los recursos en el ámbito público, como en las entidades privadas que administren fondos públicos, esta tarea la realiza de oficio o a solicitud, mediante la aplicación del Reglamento Para La Recepción y Trámite de Denuncias Para Investigación Administrativa En La Contraloría General Del Estado (2009) es así que la mencionada norma les faculta a recibir denuncias de acción popular. Es decir que la Contraloría es un actor sustancial para que las denuncias de corrupción que impliquen bienes públicos sean investigadas y de ser el caso, se determinen las debidas responsabilidades. Un punto relacionado con el Whistleblowing es que protege la reserva de la identidad del denunciante siempre que su actuar sea de buena fe.

En correspondencia con lo señalado, la tendencia es hacia un mayor reconocimiento y protección de los denunciantes, impulsado por la necesidad de combatir la corrupción principal y directa sobre el sector público, pero que a diferencia del Whistleblowing este tipo de denuncias son tramitados con mucha más formalidad y no abarcan todas posibles irregularidades que se puedan cometer en las entidades.

1.3.1. Protección de datos personales del denunciante

Los protocolos de Whistleblowing garantizan que la recopilación y el tratamiento de los datos personales del denunciante se realicen con su consentimiento informado, lo que implica proporcionar una explicación clara sobre cómo se utilizarán esos datos durante el proceso de denuncia (de la Vega & Otero, 2013), es crucial que la información del denunciante se maneje de manera segura y confidencial para proteger su identidad, pero sobre todo para prevenir represalias.

El tratamiento de datos abarca al manejo de todo dato o información personal, es fundamental diferenciar cuándo este tratamiento de datos requiere un consentimiento explícito, y cuándo, en situaciones específicas, la ley permite su procesamiento sin dicho consentimiento, es decir, cuando existe un interés público prevalente o una obligación legal que justifique el tratamiento, inclusive sin la aprobación directa del titular, estos escenarios están abordados en el Art. 7 de la Ley Orgánica de Protección de Datos Personales (2021), explica cuándo se puede tratar datos personales y en estas situaciones especiales, hay que seguir dos parámetros: proporcionalidad y finalidad. Eso quiere decir que solo se guardarán y usarán los datos que se necesitan para lograr un objetivo concreto, como por ejemplo, datos que sirvan para una denuncia que puede llevar a un juicio. Cada acción debe tener un motivo claro, así se evita cualquier uso que vaya más allá de lo necesario o que no esté permitido.

Con respecto a la protección en el tratamiento de datos del denunciante, los protocolos de denuncia interna son más flexibles para los whistleblowers (denunciantes), que para Barreiro (2024) son los delatores o alertadores de irregularidades presentadas en instituciones, estos protocolos permiten que el denunciante tenga el derecho a acceder a la información recopilada sobre él, permitiendo así la transparencia y precisión en el manejo de la denuncia pero de forma exclusiva para el denunciante.

Cuando existen denuncias mediante los canales Whistleblowing, específicamente relacionado a denuncias en las que interviene un delito contra la integridad sexual y reproductiva, la Ley Para Prevenir y Erradicar La Violencia Contra Las Mujeres (2018), en su artículo 9 numeral 6 establece la protección de datos y confidencialidad, de manera relevante si se trata de mujeres que están atravesando por una situación de vulnerabilidad, de forma especial cuando son víctimas

de violencia sexual. Esto indica que existe mayor garantía para las personas en situaciones de riesgo, de manera particular como es en el caso en análisis el denunciante es una mujer.

1.3.2. Protección de los datos del denunciado

Los protocolos deben seguir el principio de minimización de datos, asegurando que solo se recopilen y procesen los datos personales estrictamente necesarios para investigar adecuadamente la denuncia (de la Vega & Otero, 2013). Además, el denunciado tiene derechos importantes relacionados con la protección de su información privada conforme lo establece la Ley Orgánica de Protección de Datos Personales (2021). Sin embargo, estos protocolos no incluyen de forma eficiente la facultad de poder acceder a información recopilada sobre el denunciado en la denuncia y en la investigación, además de la posibilidad de acceder a la información sobre sus datos y el detalle de forma completa del que, como y para que se están usando los mismos.

La Corte Constitucional ha estudiado la delicada colisión de derechos que surge cuando se activa un mecanismo de denuncia interna y se trata de proteger los datos personales. En la sentencia N° 47-19-JD/22 (2022), se analizó la situación en que la persona que denuncia decide mantener su nombre oculto y la persona denunciada demanda datos que considera imprescindibles para preparar su defensa. Este pronunciamiento representa un avance decisivo, pues examina con rigor la tensión entre el derecho del denunciado a acceder a la información que lo compromete y la confidencialidad que los procedimientos disciplinarios internos deben respetar. En este aspecto, la Corte ha tenido que sopesar cómo garantizar un equilibrio que proteja tanto la efectividad de la protección de datos del denunciante para combatir irregularidades, como el acceso de la persona denunciada a los datos de sí mismo.

Es así que, la acción de habeas data es un mecanismo procesal esencial que ayuda a garantizar el derecho de acceso a la información personal contenida en expedientes de

investigación, este ejercicio o activación de la garantía jurisdiccional en el ámbito de las investigaciones internas, debe realizarse de manera equilibrada, salvaguardando tanto el derecho a la información del solicitante como de los terceros involucrados, finalmente contribuye a prevenir prácticas discriminatorias durante el desarrollo de las investigaciones, al garantizar que todos los solicitantes sean tratados de manera igualitaria respetando sus derechos contenidos en la Constitución al permitir la revisión de la información registrada en los expedientes.

1.3.3. Relación de los protocolos Whistleblowing y el habeas data en el Ecuador

El vínculo entre el habeas data y los protocolos de Whistleblowing se sitúa en una interrelación de derechos de protección y seguridad de datos privados, la necesidad de reportar irregularidades de forma segura y ética dentro de las organizaciones conlleva al resguardo de los datos o información personal del denunciante o afectado, la misma contenida en un expediente interno e investigativo propio de las entidades, que a su vez, contiene multiplicidad de datos incluyendo de terceras personas además del denunciado, estos protocolos o mecanismos adquieren una categoría de confidencialidad importante en estas instituciones con la finalidad de que se desarrollen de forma efectiva la ejecución de los principios de protección de datos.

Cuando se activan los protocolos de denuncias, las investigaciones internas, por su propia forma de confidencialidad, generan una tensión evidente entre derechos. Por una parte, se encuentra el imperativo de preservar el anonimato y la protección de datos del denunciante; por la otra, el deber del acusado de conocer la evidencia que le afecta. Frente a esta dicotomía, el habeas data se perfila como el mecanismo que puede articular una respuesta equilibrada. Su ejercicio permitiría que el sujeto denunciado acceda solamente a la información que le concierne, delimitando el conjunto de datos de tal manera que se salvaguarde la confidencialidad del denunciante sin sacrificar el principio de defensa. Así, el habeas data se convierte en un aspecto

garante de la coexistencia armónica de derechos en un contexto donde la investigación interna no puede renunciar a la confidencialidad sin paralelizar los derechos de las partes.

Guillén (2021) menciona que las organizaciones deben implementar un canal de denuncias interno que garantice la confidencialidad de la información y la protección de los derechos tanto del denunciante como del presunto infractor, respaldado por un marco normativo específico que ampare al denunciante. (pág. 6) Los canales de denuncia y de investigación establecen la protección de datos del denunciante y del denunciado, pero se consolida fuertemente en la protección de derechos y de confindencialidad de datos de los whisteblowers por sobre posición de los derechos del denuciado, quien tambien puede solicitar la protección de sus datos mediante los mecanismos de acción pertinetes.

En este marco de tensión entre derechos constitucionales de igual índole, resulta imprescindible abordarlos a la luz del principio pro homine, el cual impone interpretar y aplicar las normas de forma amplia, favoreciendo siempre la mayor protección posible de la persona (Pino & Quintero, n.d.) . Esto implica que, frente a un conflicto entre el derecho del denunciado a acceder a la información y el derecho del denunciante a la confidencialidad, los jueces deben optar por la solución que brinde una mayor garantía a los derechos involucrados extiendo el alcance, en lugar de limitarlos. Por ejemplo, la Corte Constitucional han ponderado estos intereses permitiendo el acceso limitado a ciertos datos por parte del denunciado, siempre que no se comprometa la identidad o seguridad del denunciante, demostrando así una aplicación concreta del principio pro persona (Sentencia: No. 47-19-JD/22, 2022).

CAPÍTULO II: METODOLOGÍA

2.1. Tipo de investigación

En el contexto de esta investigación se adoptó un enfoque cualitativo, el mismo, que se conceptualiza como una estrategia que busca comprender en profundidad las percepciones, experiencias y significados atribuidos por los actores involucrados en casos específicos (Cedeño et al., 2023), es decir que este enfoque se caracterizó por su gran interés al explorar las cualidades a profundidad y cómo se ha interpretado y experimentado la implementación de habeas data en situaciones particulares dentro de organizaciones, permitiendo capturar ciertas complejidades y matices que no podrían ser abordados únicamente a través de métodos cuantitativos.

La investigación cualitativa en este estudio se dedicó a captar datos detallados a través de técnicas como las entrevistas que fueron dirigidas a actores experimentados en el caso en cuestión o casos de similar contexto, según la doctrina, "el enfoque cualitativo es un aborde interno, subjetivo e interpretativo que permite hacer cuestionamientos sobre la realidad jurídico-social" (Nizama & Nizama, 2020). Estas entrevistas no solo buscaron obtener información, sino también exploraron las percepciones subjetivas, los dilemas éticos percibidos de los entrevistados, además, se lo empleó en el análisis de la garantía jurisdiccional, específicamente, la acción de habeas data caso (N° 17230-2018-19732, 2019) que ayudó a contextualizar y enriquecer la comprensión de la activación del habeas data.

En definitiva, mediante una metodología cualitativa, se exploró el derecho de acceso a la información personal dentro de los protocolos de denuncia interna (Whistleblowing), se analizó la aplicación de la acción de habeas data en situaciones específicas que incluyó la recolección de datos detallados mediante entrevistas a funcionarios y actores relacionados al tema, con el propósito de entender sus percepciones y experiencias en el contexto del caso real (N° 17230-

2018-19732, 2019), además se evaluó cómo se respeta el acceso a información personal y la idoneidad de la activación de la garantía jurisdiccional en dichos entornos.

2.2. Métodos de investigación

2.2.1. Descriptivo

El método descriptivo se empleó en esta investigación para describir mediante principios, análisis teóricos, normativos, jurisprudenciales y el caso en concreto de la acción de habeas data en el derecho al acceso a la información personal ante los protocolos Whistleblowing. Este método partió de principios generales establecidos por la normativa legal y jurisprudencial relacionada con el habeas data y los derechos de acceso a la información personal. A partir de estos principios, se analizó el caso específico, como el estudio del caso (N° 17230-2018-19732, 2019), además de las entrevistas realizadas a actores experimentados en la acción de habeas data, para verificar la importancia de dichos principios como medio de garantía en contextos prácticos de Whistleblowing.

2.2.2. Analítico-sintético

Se realizó un análisis detallado donde se examinó las principales dimensiones del habeas data, como el derecho a la información y la protección de datos personales.

El procedimiento analítico-sintético articula dos movimientos: tanto en análisis como la síntesis. En la fase analítica, el objeto de estudio se segmenta, de modo que cada componente se torna visible en su individualidad y especificidad. Posteriormente, en el momento sintético, esas partes, previamente esclarecidas, se reencuentran en un marco que les confiere un sentido integrado y configurador. Esta secuencialidad, según (Lopera et al., 2010), no solo proporciona un examen minucioso de los detalles, sino que, al reunirlos, permite discernir la estructura total que

los articula, promoviendo así un entendimiento más profundo del fenómeno investigado. Es útil para comprender temas complejos, ya que combina el estudio detallado y la visión global.

2.3. Técnicas e instrumentos de investigación

Para lograr el segundo y tercer objetivo de esta investigación, se realizaron entrevistas a personas idóneas y con experiencia dentro de los procesos de Whistleblowing como en la activación de la acción de habeas data. Además, se realizó un análisis profundo y sistematizado del caso en específico.

2.3.1. Entrevistas

Se llevaron a cabo entrevistas con una muestra de participantes esencial, incluyendo dos solicitantes de información personal en el proceso de Whistleblowing, los entrevistados mantuvieron la reserva de sus nombres y expusieron sus posturas sin limitaciones, "La clave radica en permitir que los participantes expresen sus puntos de vista, experiencias y percepciones de manera libre y completa" (Cedeño et al., 2023). Estas entrevistas permitieron explorar en profundidad las perspectivas, vivencias y desafíos relacionados con la implementación de habeas data en la protección del acceso a la información personal en contextos de Whistleblowing.

Las entrevistas fueron desarrolladas mediante un instrumento estratégico, el cuestionario, que permitió extraer la información más importante relacionada con el caso u obtener información relevante que no ha sido expuesta para la investigación mediante el análisis del caso en investigación "acción de habeas data", esto permitió entender y establecer como el juez ha concluido y si se estableció un beneficio o perjuicio a las partes involucradas.

Estas entrevistas se realizaron a tres sujetos clave con el objeto principal de adquirir información relevante sobre el derecho de acceso a la información personal en el contexto de los protocolos de denuncia interna:

Sujeto 1. Esta entrevista se realizó a un abogado quien actualmente es exfuncionario del CNR. El entrevistado al ser una persona que ha sido solicitante de su información personal activando la acción de habeas data ante el contexto de las denuncias internas (Whistleblowing), fue un sujeto ideal para acercarnos con mayor profundidad al tema en cuestión.

Sujeto 2. Esta entrevista se llevó a cabo con un ciudadano que se desempeña activamente como funcionario en una organización internacional humanitaria, dicha entidad gestiona prácticas de denuncia interna (Whistleblowing), en este aspecto el entrevistado recientemente gestionó de forma interna la solicitud de acceso a la información lo que le dotó de una característica importante para captar información desde otro ángulo y entender el tema en cuestión.

Sujeto 3. Esta entrevista se realizó al Dr. Ángel Valenzuela, quien ostenta el cargo de abogado especialista de los derechos humanos y de la naturaleza de la Defensoría del Pueblo en la provincia del Guayas. El Dr. Valenzuela cuenta con una gran trayectoria y experiencia particularmente en el ámbito de derechos humanos y garantías jurisdiccionales, especialmente la acción de habeas data.

Los entrevistados identificados como Sujeto 1 y Sujeto 2 mantuvieron un estatus de confidencialidad, en cumplimiento de su solicitud expresa. Esta medida se adoptó con especial énfasis para prevenir posibles represalias por parte de la organización vinculada.

2.3.2. Estudio de caso

Esta investigación se desarrolló a través del análisis de un caso específico, con el objetivo de identificar las características esenciales y predominantes que permitieron avanzar en el cumplimiento de los objetivos planteados. En este marco, se menciona que “Los estudios de caso representan una forma profunda y detallada de abordar un fenómeno o situación específica”

(Cedeño et al., 2023). El examen de casos constituye una técnica eficaz para abordar y comprender fenómenos o situaciones particulares con gran precisión.

En este contexto, se realizó el análisis sobre la acción de habeas data objeto de este estudio (N° 17230-2018-19732, 2019), resuelto por la Unidad Judicial Civil del Distrito Metropolitano de Quito. Este caso pone de manifiesto la discrepancia entre el derecho a acceder a información personal y el deber de proteger la privacidad en la información de terceros, en particular en relación de las denuncias e investigaciones internas bajo los protocolos Whistleblowing por presuntas infracciones.

2.4. Participantes (población y muestra)

El universo investigado abarcó a profesionales y actores que participan, ya sea de modo directo o indirecto, en la activación de la garantía jurisdiccional de habeas data, así como en la tramitación interna de solicitudes de acceso a información durante la gestión de los protocolos de Whistleblowing en las organizaciones. La selección de la muestra se llevó a cabo mediante un muestreo intencional que incluyó a un grupo heterogéneo de informantes clave, quienes ocupan diferentes roles y aportan perspectivas variadas dentro del campo analizado. Este enfoque garantizó la inclusión de múltiples voces y contribuyó a la riqueza de los datos recogidos.

CAPÍTULO III: RESULTADOS Y DISCUCIÓN

3.1. Resultados de las entrevistas

Tabla 1. pregunta N.-1.

1.- En su experiencia, ¿cómo se puede equilibrar el derecho del denunciado a acceder a su información personal con la necesidad de proteger la identidad y datos del denunciante dentro de los protocolos de Whistleblowing? ¿Ha enfrentado situaciones en las que este equilibrio ha sido especialmente desafiante?

Entrevistado/a	Respuesta
Abogado y exfuncionario de ONG, accionante de la Garantía jurisdiccional de acción de habeas data.	El equilibrio se obtiene mediante la aplicación rigurosa del principio de igualdad formal ante la ley, de tal forma que cada individuo, sin excepción, recibe un tratamiento idéntico ante la norma. Por imperativo, los principios constitucionales no pueden ser transgredidos por procedimientos internos, tales como los protocolos de protección de denunciantes, cuyo objetivo es preservar la confidencialidad de la identidad del informante. He tenido ocasión de observar que dicho equilibrio se quiebra cuando se antepone la instrucción del protocolo de protección de denunciantes a los derechos constitucionales. En tal caso, la persona denunciada se ve impedida de conocer los hechos que se le imputan o de identificar al denunciante, obstaculizando así su derecho al honor y, correlativamente, a una defensa efectiva.
Funcionario de ONG y solicitante de información personal.	En efecto, he atravesado una experiencia particular que, fuera de lo que pudiera suponer en principio, ha tenido un impacto notable sobre mi estabilidad psicológica y emocional. A partir de esta experiencia, sostengo que los procedimientos de protección de alertadores requieren que cualquier información documentada en una denuncia o queja interna sea objeto de una evaluación rigurosa y metódica antes de que se formulen juicios definitivos o se asigne culpabilidad. Además, el equilibrio se encontraría en que el denunciado debe tener acceso a toda la información relevante relacionada con las acusaciones en su contra, pero esto puede lograrse sin necesidad de revelar los datos personales del

	denunciante, es decir aplicando el principio de disociación preservando así su identidad y confidencialidad.
Abogado especialista de la Defensoría del Pueblo (Guayas). Abg. Ángel Valenzuela.	Habría que sopesar el derecho del denunciado a acceder a información sobre su persona dentro de un proceso sancionatorio frente al derecho de la persona denunciante que, puede ser o no, una víctima del denunciado. En este caso, haciendo un ejercicio de ponderación, tomando en consideración las posibles repercusiones o amenazas, se evitaría la identificación del denunciante. Esto no implica que el denunciado no tenga derecho a conocer las razones o motivos de la acusación, ni la negativa a acceder a información personal.

Fuente: Entrevistas, (Diciembre, 2024)
Elaborado por: Ochoa, 2024.

Dos de los entrevistados han tenido experiencias personales en la que no ha existido un equilibrio adecuado de derechos, se resalta la necesidad de respetar el principio de igualdad formal ante la ley, además se reconoce los derechos de ambas partes involucradas mediante la aplicación del principio de disociación.

Tabla 2. pregunta N.-2.

2.- ¿Ha observado si estos protocolos afectan los derechos de alguna de las partes inmersas en un proceso investigativo? De ser así, ¿qué derechos específicos se ven afectados y por qué cree que ocurre esto?

Entrevistado/a	Respuesta
Abogado y exfuncionario de ONG, accionante de la Garantía jurisdiccional de acción de habeas data.	Los protocolos internos de Whistleblowing pueden vulnerar derechos constitucionales, especialmente de la persona denunciada, como el acceso a datos personales, el principio de inocencia, la igualdad formal ante la ley y el derecho a la defensa. Las razones por la que un protocolo interno (entidad privada), aplicado sin observancia a la Constitución, vulnera derechos constitucionales son las siguientes:

	•Se adelanta criterios en perjuicio de la persona denunciada (se desvirtúa el principio de inocencia). •No se garantiza a las partes igualdad de condiciones y tampoco se les brinda los medios necesarios para la defensa, sobre todo a la parte denunciada (principio de igualdad de armas y de derecho a la defensa).
Funcionario de ONG y solicitante de información personal.	Ciertamente he experimentado restricciones a derechos fundamentales durante la fase investigativa. En particular, se ha menoscabado mi derecho a obtener información personal que concierne directamente a mi persona, pues se me han presentado diversos obstáculos para entender las motivaciones, causas y circunstancias que originaron la denuncia en mi contra. En consecuencia, se me ha negado el acceso a la información que la organización posee sobre mi persona y a las previsiones que se tienen respecto a su tratamiento y eventual utilización. Esto ha afectado mi dignidad humana, ya que me he sentido desvalorizado y en una situación de incertidumbre, y ha comprometido mi derecho a la defensa, al impedirme poseer la información indispensable para mi conocimiento y responder adecuadamente a las acusaciones.
Abogado especialista de la Defensoría del Pueblo (Guayas). Abg. Ángel Valenzuela.	Estos protocolos, en esencia, buscan prevenir repercusiones en las personas denunciantes, y a la vez, buscan incentivar que las personas puedan denunciar sin temor. Sin embargo, puede generarse cierto tipo de desequilibrio entre las partes, tomando en consideración que la entidad u organización cumple un doble rol: investigador y sancionador, que puede generar conflictos de intereses, especialmente intereses corporativos como la imagen empresarial. En este caso, el proceso no sería imparcial, siendo este un principio fundamental para garantizar el derecho al debido proceso.

Fuente: Entrevistas, (Diciembre, 2024)
Elaborado por: Ochoa, 2024.

Los entrevistados coinciden en que existen varios derechos afectados por los mecanismos de investigación interna Whistleblowing especialmente se ven afectados los derechos de aquellas personas denunciadas, entre ellos está principalmente en derecho a acceder a la información

personal, principio de inocencia, la igualdad formal ante la ley y los derechos de defensa y debido proceso.

Tabla 3. pregunta N.-3.

3.- En su opinión, ¿qué tipo de datos podrían considerarse como personales del solicitante de acceso dentro de un expediente de denuncia e investigación interna? ¿Considera relevante hacer una distinción de datos personales en la información contenida en un expediente bajo los protocolos de Whistleblowing?

Entrevistado/a	Respuesta
Abogado y exfuncionario de ONG, accionante de la Garantía jurisdiccional de acción de habeas data.	Los datos personales son aquellos que identifican a una persona: nombres, número de identidad, dirección, contacto. Son datos que cualquier persona puede solicitar porque le pertenecen. La distinción de datos personales es importante y deben ser protegidos, sin embargo, una vez abierto el trámite interno o derivado a la justicia ordinaria, estos datos deben ser revelados a las partes involucradas.
Funcionario de ONG y solicitante de información personal.	Según mi experiencia propia y las que he visto de otros casos dentro de la organización, los datos personales son aquellos que se relacionan directamente con la persona afectada y que tienen un impacto sobre ella. Sí es importante hacer una distinción entre los tipos de datos, especialmente si deben manejarse de forma pública. Sin embargo, en un contexto interno, los datos no sensibles, como los nombres del denunciante, deberían estar disponibles para identificar el origen de la información de la denuncia. Esto permitiría que la organización actúe de forma adecuada y en caso de represalias, con su facultad protectora debería garantizar la representación legal del denunciante, evitando vulneraciones de derechos para todas las partes.
Abogado especialista de la Defensoría del Pueblo	La información que se considera personal incluye datos que están relacionados directamente con la privacidad y los derechos individuales, como una historia clínica, que solo puede compartirse con la autorización del paciente. En el

(Guayas). Abg. Ángel Valenzuela.	marco de un procedimiento de denuncia regido por estos protocolos, es imperativo diferenciar, con la máxima precisión, la información amparada por la normativa de protección de datos, tales como datos confidenciales o sensibles. Su tratamiento ha de realizarse con la más estricta cautela, de tal manera que se respete la normativa vigente sobre acceso, tratamiento y custodia, asegurando la confidencialidad que les es inherente, y eludiendo, de este modo, cualquier conculcación de derechos constitucionales.

Fuente: Entrevistas, (Diciembre, 2024)
Elaborado por: Ochoa, 2024.

Los interrogados coinciden en que los datos personales son aquellos en que lo hacen identificables o que se relacionan de forma directa con una persona, además de aquellos datos que guardan relación con la privacidad y los derechos individuales, además consideran que si debe existir distinción de datos para que estos sean protegidos especialmente si se manejan de forma pública, además, se reconoce que existen datos sensibles que su protección debe ser garantizada como lo establece la Constitución.

Tabla 4. pregunta N.-4.

4.- ¿Percibe usted que existen diferencias en la gestión al acceder a la información cuando las denuncias involucran delitos penales, como el acoso sexual, en contraste con otras denuncias internas? ¿Cuáles son los argumentos o consideraciones que respaldan estas diferencias en el manejo de la información?

Entrevistado/a	Respuesta
Abogado y exfuncionario de ONG, accionante de la	Los delitos deben ser tratados de manera diferenciada, derivando las denuncias a la Fiscalía para su investigación. Sin embargo, en mi experiencia, la institución que aplicó el Whistleblowing no dio un tratamiento especial ni presentó denuncias formales ante las autoridades competentes.

Garantía jurisdiccional de acción de habeas data.	Las instituciones privadas que manejan estos protocolos deben anunciar a la parte denunciada sobre toda la información (hechos e identidades) para que ejerza su defensa. Y con más razón si estos casos se judicializan, puesto que en una investigación o proceso penal se debe contar con los datos de todas las personas vinculadas.
Funcionario de ONG y solicitante de información personal.	No existen diferencias significativas porque los protocolos garantizan principalmente la confidencialidad de todas las denuncias y los procesos de investigación. Digo que no hay diferencias porque he visto que por este tipo de protocolos internos manejados sin un debido proceso he visto desvirtuado muchos derechos de mis compañeros los cuales han tenido que salir de la organización por temor.
Abogado especialista de la Defensoría del Pueblo (Guayas). Abg. Ángel Valenzuela.	Si existe una diferenciación en la gestión de información en este tipo de conducta (delitos y contravenciones contra la integridad sexual) y ésta diferencia obedece a la protección de la presunta víctima y a su derecho a no ser revictimizada.

Fuente: Entrevistas, (Diciembre, 2024)
Elaborado por: Ochoa, 2024.

Del análisis de estas respuestas se desprende, que los protocolos de Whistleblowing garantizan la confidencialidad de todas las denuncias internas, independientemente de si estas tienen o no carácter penal. De tal modo, la revisión de los datos personales incorporados en una denuncia se halla limitada no tanto por la naturaleza del ilícito, sino porque las políticas de denuncia de irregularidades consagran la confidencialidad como norma general aplicable a todos los casos. No obstante, los entrevistados coinciden en que, cuando surgen indicios de conductas delictivas, la información ha de ser gestionada de forma puntual, procediendo a elevar la denuncia a la Fiscalía con el fin de que inicie la investigación correspondiente. En este proceso, se permite

el acceso no solo a los datos personales, sino también a los hechos denunciados y a la identidad de los denunciantes.

Tabla 5. pregunta N.-5.

5.- ¿cómo puede influir la acción de habeas data en el manejo del acceso a la información personal de los denunciados dentro de los protocolos de Whistleblowing? ¿Considera que esta acción puede tener un impacto positivo o negativo en la protección de los derechos de todas las partes involucradas?

Entrevistado/a	Respuesta
Abogado especialista de la Defensoría del Pueblo (Guayas). Abg. Ángel Valenzuela.	La acción de habeas data influiría principalmente en el aspecto del conocimiento de la información relacionada directamente con el denunciado y que se está tratando en un proceso, sobre todo de forma positiva dentro de un proceso que se haya accedido a información confidencial y que esta información accedida pueda generar un impacto negativo en la persona denunciada, y el habeas data permitiría que dicha información sea eliminada o que se garantice la confidencialidad de la misma.

Fuente: Entrevistas, (Diciembre, 2024)
Elaborado por: Ochoa, 2024.

El habeas data resulta especialmente positivo para el denunciado, ya que le permite conocer la información que está siendo tratada en un proceso y que podría tener un impacto negativo en su contra. Este derecho le otorga la posibilidad de solicitar la eliminación de dicha información o exigir garantías de confidencialidad para proteger su privacidad.

Tabla 6. pregunta N.-6.

6.- ¿Cree usted que la acción de habeas data es un mecanismo adecuado para garantizar el acceso a información personal en el marco de los protocolos de denuncias internas, particularmente en relación con los datos contenidos en un expediente de denuncia e investigación?

Entrevistado/a	Respuesta
Abogado y exfuncionario de ONG, accionante de la Garantía jurisdiccional de acción de habeas data.	Sí, la garantía de acción de habeas data es la vía constitucional efectiva para garantizar el acceso a la información personal de la persona que la requiere, así como de todas las circunstancias de tiempo, lugar y modo en que acaecieron los hechos que se denuncian. Sin embargo, esta acción es limitada para conocer los datos personales de otras personas involucradas, porque justamente no corresponden a la información personal de la persona que ha presentado esta acción jurisdiccional. En síntesis, la acción de habeas data es útil para el acceso a la información personal del accionante, o sea del que presenta la acción ante la justicia constitucional, pero es ineficaz para acceder a los datos de otras personas.
Funcionario de ONG y solicitante de información personal.	Actualmente me encuentro todavía en mis labores dentro de la organización y enfrentando un proceso de denuncia interna, por lo cual estoy esperando respuesta y en el caso que no se me respeten mis derechos tendré que activar un recurso de habeas data porque lo considero adecuado para solicitar la eliminación de mi información que afecte mis derechos constitucionales y que se encuentre contenida en el expediente de la organización.
Abogado especialista de la Defensoría del Pueblo (Guayas). Abg. Ángel Valenzuela.	Sí es adecuado, pero la Corte Constitucional del Ecuador se ha pronunciado en varias sentencias, respecto a la garantía jurisdiccional de la acción de protección como la garantía más adecuada para el acceso a información que se encuentra dentro de un expediente de denuncia e investigativo, sea administrativo o judicial, porque no solo contiene información personal sino que guarda relación con el derecho al debido proceso y el derecho a la defensa.

Elaborado por: Ochoa, 2024.
Fuente: Entrevistas, (Diciembre, 2024)

De acuerdo con las personas consultadas, la acción de habeas data se percibe como un recurso adecuado y eficaz para obtener información personal y datos concretos vinculados al denunciado, así como para su posterior cancelación en caso de que así se requiera. No obstante, se observa un desacuerdo en el momento en que se busca acceder a datos de mayor envergadura, particularmente a la documentación que integra un expediente de denuncia o de investigación, en cuyo caso el mecanismo más pertinente es la acción de protección.

Tabla 7. pregunta N.-7.

7.- ¿Cómo se asegura el derecho de acceder a la información en casos de denuncias de acoso sexual u otras infracciones dentro de los protocolos de denuncia, sin poner en riesgo la confidencialidad de las partes involucradas, especialmente en lo referente al resguardo de datos personales?

Entrevistado/a	Respuesta
Abogado y exfuncionario de ONG, accionante de la Garantía jurisdiccional de acción de habeas data.	Se asegura denunciado ante la Fiscalía, que es la autoridad encargada de investigar y, de ser necesario, acusar al denunciado. En este proceso, tanto el denunciante como el denunciado tienen acceso a toda la información del expediente, incluidos los datos personales de las partes, garantizando al mismo tiempo la confidencialidad que se aplica solo para terceros, no para las partes ni sus defensas técnicas.
Funcionario de ONG y solicitante de información personal.	Considero que la información relacionada con denuncias de acoso sexual debe manejarse con extrema delicadeza. He sido testigo de situaciones en las que colegas acusados de conductas impropias no lograron obtener datos fundamentales para su defensa, lo que los colocó en una posición de indefensión que los presentaba, de forma automática, como culpables. Este fenómeno se produjo porque la institución optó por no canalizar los expedientes a las autoridades judiciales competentes, comportándose a la vez como acusador y tribunal y ventilando los asuntos en su propio criterio. Sostengo que los derechos de las personas denunciadas no deben quedar comprometidos en aras de preservar la confidencialidad de los denunciantes; en realidad,

	es indispensable que ambos derechos se ponderen y protejan en igual medida.
Abogado especialista de la Defensoría del Pueblo (Guayas). Abg. Ángel Valenzuela.	Los protocolos de denuncia deben guardar armonía con la legislación interna que establece información de carácter confidencial, como la Ley del Paciente, entre otros, así como garantizar el acceso toda la información que sea necesaria para que la parte denunciada a fin de que pueda conocer esta información pueda ejercer sus derechos en pleno conocimiento de la misma, como el de la defensa, y a la vez, evitar que la denunciante pueda caer en revictimización o repercusiones.

Fuente: Entrevistas, (Diciembre, 2024)
Elaborado por: Ochoa, 2024.

Los entrevistados sostienen que el derecho de acceso a información en denuncias de acoso sexual u otras infracciones bajo los mecanismos de Whistleblowing queda garantizado cuando todo el material contenido en la queja se comunica a la Fiscalía. De esta forma, la naturaleza confidencial de la información se restringe a la divulgación pública o a terceros ajenos, sin extenderse a las partes que intervinieron en la denuncia. Adicionalmente, los procedimientos de denuncia deben alinearse con la normativa nacional, la cual prescribe el trato confidencial de los datos, al tiempo que reconoce a las partes el derecho a acceder y conocer dicha información con el fin de ejercer plenamente sus derechos.

Tabla 8. pregunta N.-8.

8.- ¿Cómo considera que se puede equilibrar la necesidad de transparencia en la gestión de denuncias de acoso sexual u otras infracciones con la protección de los derechos de las supuestas víctimas y denunciantes, especialmente en lo que respecta a la confidencialidad y el acceder a la información?

Entrevistado/a	Respuesta
Abogado y exfuncionario de ONG, accionante de la Garantía jurisdiccional de acción de habeas data.	De ninguna manera este tipo de casos, u otros que involucren delitos se los debe manejar bajo los preceptos de los protocolos por cuanto las instituciones privadas que aplican el Whistleblowing no son competentes para conocer y tramitar los casos de esta naturaleza. Es por esto que para que exista transparencia es obligatorio remitir estos casos a las autoridades competentes, como la Fiscalía. Una vez en esta instancia, la confidencialidad se debe aplicar pero únicamente a terceros, mientras que las partes involucradas tienen pleno acceso al expediente, incluida la información y datos personales relacionados con la investigación.
Funcionario de ONG y solicitante de información personal.	Se debería equilibrar principalmente respetando el derecho del denunciado a no tener un bloqueo a la información que le concierne, la organización debe actuar como garante de derechos y no dejar indefenso al denunciante, lo que permite garantizar los derechos de todas las partes inmersas. Para asegurar la transparencia en el manejo de estos protocolos la información debe estar al alcance desde los primeros momentos de la activación del mismo, en casos en los que las infracciones no sean graves, en otros casos más graves se debería remitirse a la información en la fiscalía para su correspondiente investigación.
Abogado especialista de la Defensoría del Pueblo (Guayas). Abg. Ángel Valenzuela.	Este tipo de denuncias pueden generar potenciales vulneraciones a derechos inherentes a la dignidad humana, como el honor y buen nombre, integridad física y psicológica, entre otros, tanto de las personas denunciantes como de las personas denunciadas. El acceso a la información de estos procesos debe pertenecer solo a la esfera de las partes, y no de acceso al público en general.

Fuente: Entrevistas, (Diciembre, 2024)
Elaborado por: Ochoa, 2024.

Para garantizar la transparencia en la gestión de los protocolos de Whistleblowing, la información debe estar disponible para el denunciado desde los primeros momentos de su

activación, siempre que las infracciones no sean graves. En casos más graves, la información debe ser remitida a la Fiscalía para su correspondiente investigación, ya que este ente sería el encargado de equilibrar la transparencia, la confidencialidad para el denunciado y el denunciante.

Por otro lado, las instituciones privadas que implementan protocolos de Whistleblowing no son competentes para tratar casos de naturaleza penal. Esto podría derivar en vulneraciones a la dignidad humana en lo que corresponde al honor, buen nombre, y la integridad física y psicológica de las partes involucradas.

Tabla 9. pregunta N.-9.

9.- ¿Cómo valora la decisión de activar la garantía de habeas data para obtener acceso a su información personal? ¿Percibe algún desafío particular al hacer valer esta garantía bajo los parámetros Whistleblowing?

Entrevistado/a	Respuesta
Abogado y exfuncionario de ONG, accionante de la Garantía jurisdiccional de acción de habeas data.	La valoración es positiva, porque la garantía de acción de habeas data es en realidad una vía sumamente efectiva para garantizar el acceso a la información personal que me fue denegada. El reto es que los protocolos (Whistleblowing) deben guardar armonía con la norma suprema (Constitución), se debe entender que estos protocolos sirven para generar una alerta temprana y una ruta efectiva para atender una denuncia, pero no para "tramitarlos" internamente, mucho menos para vulnerar derechos constitucionales de las personas involucradas.
Funcionario de ONG y solicitante de información personal.	La garantía de habeas data es un recurso importante, aunque su activación depende de la situación particular de cada denunciado. Conforme mi experiencia la organización practica un hermetismo que obstaculiza el acceso a la información que me concierne, circunstancia que me lleva a sostener que dicho acceso es un derecho fundamental.

	Defenderé la posibilidad de invocar dicha garantía cuando juzgue que la información me perjudica, particularmente si la denuncia contiene elementos que lesionan de manera grave mi inocencia, mi honra o mi buen nombre. En tal supuesto, no vacilaré en recurrir a la vía jurisdiccional para exigir el respeto a mis derechos, pedido que incluiría la restitución por los daños efectivos que la permanencia de tales datos me haya causado. No percibo grandes desafíos en hacer valer esta garantía, ya que los derechos están amparados por la Constitución, lo fundamental es identificar correctamente el procedimiento jurisdiccional adecuado para ejercer estos derechos en cada caso en particular.
Abogado especialista de la Defensoría del Pueblo (Guayas). Abg. Ángel Valenzuela.	Si bien la garantía de habeas data es la garantía adecuada para acceder a información de carácter personal y tiene un valor fundamental para conocer la información que identifique a la persona solicitante, pero considero que la acción de protección sería el camino más idónea para acceder a información dentro del procesos administrativos y/o judiciales, puesto que la falta de acceso a ellos limita el derecho a la defensa eficaz. Un desafío es poder identificar y determinar los datos que pueden hacer identificable a una persona, especialmente dentro de un expediente investigativo.

Fuente: Entrevistas, (Diciembre, 2024)
Elaborado por: Ochoa, 2024.

Según los entrevistados, la valoración de activar la acción es positiva, particularmente cuando dicho acceso ha sido previamente negado por la entidad responsable del tratamiento de datos, directamente con el acceso a datos que identifican al titular y que afectan su inocencia, honra o buen nombre, además de adecuado para solicitar la eliminación de estos datos cuando afectan a su titular. En este contexto, el desafío radica en identificar con precisión cuáles datos son tomados en consideración como personales, es decir los que permitirian identificar a cierta persona dentro de la información contenida en un expediente. Sin embargo, si el objetivo principal es acceder a la

información para ejercer el derecho a la defensa, resulta más pertinente recurrir a otros medios legales.

3.2. Análisis del caso habeas data (N° 17230-2018-19732, 2019)

A través de este análisis, se va a revisó los siguientes aspectos: marco constitucional del derecho de acceso a la información personal, principios fundamentales vinculados al habeas data, alcance y límites del habeas data, pertinencia de los datos solicitados mediante habeas data.

3.2.1. Resumen de la garantía jurisdiccional de acción de habeas data caso N° 17230-2018-19732

El presente análisis jurídico se centró en el caso de habeas data (N° 17230-2018-19732, 2019), resuelto por la Unidad Judicial Civil del Distrito Metropolitano de Quito en 2019. Este caso pone de manifiesto la tensión entre el derecho de acceso a la información personal y el compromiso de proteger la privacidad de terceros, en particular en el contexto de investigaciones internas bajo los protocolos Whistleblowing por presuntas infracciones laborales.

3.2.1.1. Hechos del caso

Un trabajador, al ser objeto de una investigación interna por presuntas irregularidades (mal manejo de recursos humanitarios y conductas de acoso sexual), solicitó acceso al expediente correspondiente. La organización, por su parte, se negó a proporcionar la información completa alegando la necesidad de mantener a salvo la identidad del denunciante y la confidencialidad del proceso.

3.2.1.2. Posición del accionante

El trabajador argumentó que su derecho a la información había sido vulnerado, solicitando específicamente detalles sobre el tiempo, lugar y modo en que ocurrieron los actos reportados, así

como la identidad de los denunciantes y cualquier documento que se le relacione y que incluya información sobre el reporte de infracción al código de conducta de la organización.

3.2.1.3. Posición del demandado

La organización defendió su negativa alegando la responsabilidad de mantener en reserva la identidad del denunciante y garantizar la confidencialidad del proceso de investigación. Asimismo, argumentó que el trabajador había perdido el interés legítimo en la información al presentar su renuncia.

3.2.1.4. Decisión judicial

La jueza resolvió parcialmente a favor del accionante, ordenando la entrega de la información relacionada con los hechos denunciados y determinados en "tiempo lugar y modo" con respecto a datos, informes y comunicaciones referentes al accionante, pero excluyendo cualquier dato que pudiera revelar la identidad de los denunciantes (Sentencia N° 17230-2018-19732, 2019).

Este caso plantea diversas interrogantes sobre la aplicación del habeas data y sobre los límites del derecho a la información de carácter personal. ¿Hasta qué punto el derecho a la privacidad de los denunciantes debe prevalecer sobre el derecho del acusado a conocer información que se relaciona de forma personal en su contra? ¿Cómo se determina que la información del "tiempo, lugar y modo" de los hechos se relacionan con el accionante como sus datos personales?

En la sentencia, la Dra. Carmen Romero Ramírez determina que la parte demandada en la acción jurisdiccional no está autorizada a invocar, en este caso, la confidencialidad de la información y la protección del delator si tal invocación repercute en la vulneración de derechos de rango constitucional. Asimismo, enfatiza la primacía del principio de igualdad entre los sujetos

procesales y recuerda que el recurso de habeas data tutela no solo la privacidad, sino también la dignidad y la integridad psíquica de la persona, habida cuenta de que el procedimiento investigador vinculado a la denuncia interna puede menoscabar de manera seria su honra y su bienestar emocional (Sentencia N° 17230-2018-19732, 2019).

3.2.2. Resultados del análisis de la acción de habeas data caso N° 17230-2018-19732

En el marco de la garantía jurisdiccional de habeas data en análisis, se reconoce, conforme a la normativa constitucional y jurisprudencial, los derechos de los que figuran como titulares legales de datos personales por parte del juzgador, tanto en relación con el denunciante como con el denunciado. No obstante, se ha enfatizado principalmente sobre el derecho del accionante a acceder y conocer su propia información, dado que constituye una característica intrínseca de la acción propuesta, esto se realizó sin desatender la protección de datos que ampara al denunciante en lo que respecta a la confidencialidad.

En este sentido, se ha evidenciado en el caso, una aplicación de confidencialidad absoluta, manifestada en la negación del derecho de acceso a la información personal por parte de la organización, el mismo que pretende proteger los datos de carácter personal especialmente aquellos catalogados como sensibles, pero también el cuidado del denunciante con la finalidad de evitar represalias. Sin embargo, se expone que la confidencialidad, siendo un derecho legal de los que fungen como titulares de datos dentro de los documentos manejados por los protocolos internos, no puede ser utilizada como justificación para afectar los derechos de acceso a los datos personales del titular, particularmente cuando la confidencialidad entra en conflicto con derechos irrenunciables, tal como lo establece la garantía de habeas data y la Ley Orgánica de Protección de Datos Personales (LOPDP).

Por tanto, el recurso de habeas data ha sido invocado ante la negativa de la entidad a facilitar información o documentación concerniente a quien lo interpone. Tal omisión ha motivado la necesaria intervención del accionante en ejercicio de la tutela judicial despertada por la mencionada garantía.

Conforme a lo anterior, el órgano jurisdiccional ha sometido la controversia a la luz de los preceptos constitucionales y de la doctrina constitucional sobre el derecho de acceso a la información, determinando el deber de transparencia y el derecho del peticionario a obtener los datos de carácter personal que obran en su contra, así como a ser informado sobre el contexto y la finalidad del tratamiento.

En el presente asunto se ha operado con los principios que nutren la acción de habeas data, lo que ha conducido a la consecución de una solución equilibrada para las partes. Se ha puesto de relieve la técnica de disociación, empleada para prevenir una eventual afectación de los derechos del denunciante en escenarios de denuncia interna, y que permite, de este modo, armonizar los derechos de todos los implicados.

Por otro lado, se evidencia que el accionante no dirige su acción exclusivamente a los datos personales que le afectan directamente o le conciernen, sino que también solicita información relativa al denunciante (whistleblower). Además, su pretensión se orienta hacia objetivos que, en cierta medida, difieren de la naturaleza propia del habeas data, como es el acceso y la consecuente protección de los datos personales. Esto demuestra que dicha solicitud carece de pertinencia respecto al objeto de la garantía misma.

De igual forma, el accionante, más que perseguir como finalidad la protección, intenta obtener información de carácter general con el propósito de ejercer su derecho de defensa, tal como consta en el caso en análisis. Es decir, mediante la activación del habeas data en análisis, no solo

se solicita datos o información referente y exclusivamente a su titular, tal como lo establece en sus parámetros la Constitución y la jurisprudencia de Corte Constitucional, si no que se desvía al solicitar el acceso a nombres, apellidos y documentos de identidad de denunciantes o whistleblowers, con la finalidad de garantizar el derecho del denunciado a conocer quién originó las acusaciones y preparar una defensa. Este acceso, sin embargo, resulta improcedente conforme a la normativa vigente y según lo resuelto por la juzgadora, dado que el habeas data no ampara el acceso a información de terceros.

Así mismo, en la solicitud presentada, se requiere información sobre los factores de tiempo, lugar y modo determinantes de los hechos denunciados, argumentando que estos elementos guardan relación con el accionante y constituyen datos personales. La juzgadora ha autorizado este acceso al considerar que dicha información califica como personal, siempre que la información aluda directamente al accionante o guarde relación con su persona, sin que ello implique vulneración de otros derechos (Sentencia: No. 47-19-JD/22, 2022).

3.3. Discusión

Una vez realizado el análisis de la teoría, la normativa relativa al habeas data y al derecho de acceso a la información personal, junto con el estudio de la jurisprudencia de la Corte Constitucional, las experiencias y perspectivas recogidas en las entrevistas, y el examen del caso específico, se procede a contrastar dicha información con el fin de contestar la pregunta guía de la presente investigación: ¿De qué manera la acción de habeas data garantiza el derecho de acceso a la información personal sin vulnerar el derecho a la protección de datos personales del denunciante, en el contexto de los protocolos de denuncia interna Whistleblowing, según lo demuestra el análisis del caso No 17230-2018-19732? Así mismo, este capítulo favorece el logro de los objetivos establecidos en el presente proyecto de investigación.

El caso en estudio demuestra que la pretensión de acceso judicial mediante la garantía jurisdiccional, por parte del accionante son: el acceso a la denuncia e informes o documentos relativos a su persona contenidos en el expediente de investigación, además de los datos de los denunciantes, es decir no solo se centra en sus datos personales, en este sentido, la jueza acepta de forma parcial la garantía y reconoce el derecho exclusivo del titular (accionante HD), aplica la norma garantista con respecto al acceso de los datos referentes a su persona conforme lo solicitó, ordenando su entrega para garantizar su protección.

El habeas data, aun centrado en la protección de datos personales, se enfrenta a una cuestión compleja cuando lo que se trata es un conjunto amplio de información en lo que la calidad de "personal" presenta ambigüedades. En tales situaciones, la solicitud de acceso puede abarcar fragmentos de información que, a pesar de su pertinencia, caen bajo la salvaguarda constitucional de la intimidad. De ahí que sea imperativo delimitar con precisión el alcance de la noción de "dato personal", entendiéndolo como cualquier dato que se relacione, directa o indirectamente, con un individuo singular, o que, a partir de su combinación, permita una identificación inequívoca de la persona a la que se refiere. Esta distinción es esencial debido a que permite que solo se acceda a la información que corresponde al solicitante sin vulnerar los derechos otros.

La Ley Orgánica de Protección de Datos Personales (2021), estipula que el dato personal es aquel que logra identificar a un sujeto. Además, la Corte Constitucional en su Sentencia: No. 47-19-JD/22 (2022), citó a la referente ley y se pronunció dentro del caso en análisis, menciona que la información contenida en un expediente de investigación y una denuncia contienen diversidad de datos correspondientes a distinta clase, por lo que realiza una distinción de datos, dejando claro que la información susceptible de acceso mediante acción de habeas data sería la que permite que un sujeto se haga identificable.

En el caso en estudio se observa que existe una desviación o cierta desnaturalización en la pretensión del sujeto activo, debido a que, dentro de la solicitud de información o acceso a reportes relacionados al accionante, además de los datos de terceros, incluye el objetivo de conocer el "tiempo, lugar y modo" de los supuestos incidentes cometidos y denunciados, mismo que no son pertinentes mediante la acción o no dan cabida, ya que no son datos del solicitante (Sentencia: No. 47-19-JD/22, 2022). Esta pretensión la fundamenta en el uso que va a dar a los datos pretendidos para hacer valer su derecho a la defensa frente a las acusaciones.

En este contexto, la Corte Constitucional ha establecido reglas claras para la activación del habeas data y señala que el petitorio debe estar dirigido exclusivamente a datos personales como lo es la naturaleza propia de la acción y que su alcance debe garantizar que se cumplan los objetivos del habeas data de manera eficaz y dentro de los parámetros legales establecidos (Sentencia 182-15-SEP-CC, 2015). Sin embargo, en este caso se observa que la pretensión del accionante excede este marco al incluir la solicitud de información de un tercero (el denunciante), lo cual desnaturaliza el propósito de la acción con la finalidad de obtener información para su recurso de defensa en un procedimiento sancionatorio.

El titular de los datos ha ejercido su derecho sobre su información personal, mediante el elemento de acceso, el mismo que está integrado dentro de los componentes fundamentales del habeas data, conforme lo expresa la doctrina a través de su autor Garrido (2024), y de conformidad con la Corte Constitucional en su jurisprudencia con la Sentencia 182-15-SEP-CC (2015) la misma, menciona que dentro de los componentes se destaca el derecho de acceso que proporciona la categoría de habeas data informativo, el cual constituye un punto fundamental para que el titular pueda comprender qué tipo de datos personales están siendo objeto de tratamiento, entendiéndose como un mecanismo que asegura la protección de los datos personales mediante la garantía

jurisdiccional para proteger el derecho del titular a conocer y determinar el uso de sus datos personales de manera efectiva. Por lo tanto, resulta indispensable que el interesado posea una comprensión completa de sus datos antes de emprender el ejercicio de control sobre los mismos.

Este derecho concede al solicitante la capacidad de recoger información exhaustiva sobre sus datos personales, abarcando la naturaleza de la información que se posee, los medios a través de los cuales fue obtenida y la finalidad que sustenta su tratamiento. Como ha señalado la Corte Constitucional, esta perspectiva se apoya en el principio de acceso y en el derecho a la transparencia. Sin embargo, la misma Corte también menciona el "quién" que no aplicaría al sentido de la garantía porque hace referencia a características que pueden permitir la identidad del sujeto que la obtuvo, no aplicable según la naturaleza del habeas data. En el caso analizado, el sujeto activo de la acción ejerce esta prerrogativa al solicitar información bajo estas directrices, esto se encuentra en total consonancia con lo estipulado en el artículo 92 inciso primero de la Constitución (2008), que garantiza el derecho del titular a conocer el origen de sus datos, su finalidad y el uso que se les está dando.

Por otro lado, la protección de datos personales no se limita únicamente al acceso o a la información, la rectificación o supresión de información, sino que trasciende más allá, al constituirse el habeas data en una garantía frente a posibles perjuicios en el ámbito íntimo o personal del titular, debido a que al analizar el contenido de informes, reportes o denuncias generados en el marco de mecanismos de Whistleblowing, estos pueden contener información sensible y afectar a la honra y el buen nombre de la persona involucrada.

Las Naciones Unidas en su Declaración Universal de los Derechos Humanos determina la afectación a la privacidad o intimidad de las personas, misma que se concreta por las injerencias que lesionan la honra y la reputación de un individuo (Naciones Unidas, 1948), en concordancia

con la Constitución (2008) que establece en el artículo 66 numeral 18 que hace alusión al derecho que tienen las personas tanto al honor y buen nombre. Por tal razón, el habeas data no solo implica la protección frente a vulneraciones directas a los datos personales, sino que también conlleva la protección de los datos cuando estos afectan al honor de los individuos en el manejo de su información personal. Esta protección es especialmente relevante en el entorno de la información tratada mediante los canales Whistleblowing, específicamente cuando la información contiene denuncias sobre delitos que no han sido judicializadas y afectan la reputación y prestigio del denunciado.

En las entrevistas se identifica, que la información obtenida sobre el posible cometimiento de un delito y no remitida a la fiscalía puede vulnerar el derecho al buen nombre o prestigio del denunciado. Esto puede ocurrir debido a que dicha información, es manipulada o tratada por terceros vinculados a la organización durante el proceso de investigación, generando afectaciones morales a los denunciados, debido a que estas personas son consideradas culpables de manera anticipada, lo que también impacta negativamente en su derecho a la defensa frente a las acusaciones.

En este sentido, la Sentencia No. 2064-14-EP/21 (2021) de la Corte Constitucional resulta particularmente relevante, al ampliar el alcance del habeas data como un instrumento no solo de control informativo, sino también de protección integral en relación con la dignidad humana, al reconocer que los datos personales, en su sentido más amplio, están íntimamente vinculados con derechos como la honra y la identidad personal. En este contexto, el cuidado de los datos no aplica solo para los denunciantes sino también a los denunciados, garantizando el pleno respeto de todos los derechos inherentes a sus titulares.

Por otro lado, un aspecto negativo es la ausencia, dentro de la legislación ecuatoriana, de una norma específica que regule los protocolos para el manejo de casos de Whistleblowing en las organizaciones, esta falta de normativa no otorga a las entidades la facultad de negar derechos relacionados con los datos personales de sus titulares, ya que estos procesos, al encontrarse en fase administrativa de investigación, aún no han sido judicializados.

En las entrevistas realizadas, se evidencia que se presentan varios casos de solicitud de acceso a datos de carácter personal, en instituciones similares al caso en estudio, mismas que se han propuesto para acceder tanto administrativamente como judicialmente, solicitando el acceso a la información relacionada a su titular contenida en los expedientes manejados mediante protocolos de Whistleblowing y otros procesos similares, la información requerida se relaciona al titular pero con el objeto de conocerla para usarla de forma informativa y como medio de defensa especialmente en casos que involucran acusaciones graves, como el acoso sexual.

Los entrevistados por un lado están en pleno conocimiento de que el habeas data no corresponde para los datos que identifiquen a otros, además, consideran que la confidencialidad de datos no debe aplicarse a las partes inmersas dentro de un proceso administrativo iniciado por denuncia de delitos, más bien indican que se debería judicializar para garantizar el principio de igualdad de armas y de derecho a la defensa, lo que en instancia permitiría que se obtenga acceso a toda la información referente al caso denunciado, por lo tanto, consideran que la confidencialidad se encuentra vinculada más hacia lo público que a las partes intervinientes.

A este respecto, en el caso en específico habeas data (N° 17230-2018-19732, 2019), la denuncia recibida mediante la activación del protocolo Whistleblowing no ha sido judicializada, por tal razón, existen múltiples obstáculos para acceder a esta información, debido a las políticas

internas de confidencialidad adoptadas por las instituciones, cuyo propósito es proteger la identidad y los datos personales de los denunciantes.

En relación con la información protegida del denunciante (whistleblower), dicha información también se encuentra amparada por la Constitución (2008), con mayor razón cuando se trata de información sensible vinculada a personas en situación de movilidad humana, consideradas como grupos prioritarios investidos de protección especial según lo establece el artículo 41 de la norma suprema.

En el supuesto examinado, la denunciante, mujer que constituye una posible víctima de hostigamiento sexual, disfruta de un régimen reforzado de protección respecto a la reserva de su información personal, conforme al inciso 6 del artículo 9 de la Ley Orgánica Integral Para Prevenir y Erradicar La Violencia Contra Las Mujeres (2018), dicha disposición reconoce el derecho a la confidencialidad como medio para preservar su privacidad y garantizar su integridad, haciendo hincapié en la obligación de las autoridades y de los operadores jurídicos de manejar la información con el máximo celo y de limitar su divulgación a los estrictamente necesario para la investigación y la protección de la víctima. Sin embargo, esto no faculta para que el denunciado no pueda acceder a sus propios datos, de las entrevistas realizadas, se identifica la problemática en el acceso y comprensión sobre los datos de los titulares (denunciado) dentro de los mecanismos de denuncia e investigación organizacional, esta falta de transparencia dificulta el equilibrio entre los derechos de los titulares de datos personales contenidos en un expediente, en particular, cuando los procesos investigativos involucran delitos de índole sexual que deberían ser canalizados exclusivamente a través de los organismos estatales competentes, como la Fiscalía, que tiene la responsabilidad legal de llevar a cabo investigaciones y acusaciones en caso de hallar indicios de

delitos. Es decir, que las organizaciones, al actuar como juez y parte, comprometen la imparcialidad y la adecuada administración de justicia.

De esta manera, la información relacionada con la recopilación de datos referente a un delito de índole sexual implica que la confidencialidad se aplique para el público y no para las partes inmersas en un proceso de esta naturaleza, según lo mencionan los entrevistados, mismos que consideran que el acceso debe ser directo a la información relacionada no solo sobre datos personales sino también sobre lo concerniente a la denuncia y demás detalles como la fuente de la que se obtuvo, su manejo o tratamiento.

Ahora bien, bajo el marco de la confidencialidad establecida por los protocolos de denuncia e investigación organizacional, no debería existir restricción alguna para que el titular acceda a sus propios datos personales contenidos en dichos procesos, más bien, sí se determina la confidencialidad como medio de protección de datos del denunciante, y en el caso específico datos de una persona en condición de desplazamiento humano. Es decir, que se afecta el principio de transparencia, el mismo que se vincula directamente con el acceso y conocimiento, este principio garantiza no solo la adecuada custodia de dichos datos, sino también la accesibilidad sencilla y clara a la información relacionada a una persona, permitiendo que los titulares puedan comprender y gestionar su uso de manera informada, tal como lo menciona el autor (Quiroz, 2016).

Así mismo, la confidencialidad como principio está expresamente recogido en el artículo 10, literal g, de la Ley Orgánica de Protección de Datos Personales (2021), como uno de los pilares de la administración de datos personales. Dicho manejo, exige de la autorización del titular, conforme lo dispone el en su articulado 66 numeral 19, que en su parte pertinente menciona "(…) La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley." (Constitución, 2008).

Es así como, la norma establece claramente el derecho de las personas al resguardo o confidencialidad de sus datos personales, esta disposición resalta la importancia de la privacidad de los datos de los individuos y permite que su uso no se realice sin el consentimiento adecuado, ni se divulgue de manera inapropiada.

En las entrevistas realizadas, se observa que la confidencialidad de los datos e información del denunciante y del expediente, toma gran fuerza dentro del contexto de los protocolos de Whistleblowing. El principio aludido, contemplado en los sistemas de gestión de denuncias organizacionales, persigue la salvaguarda de la identidad del informante, con la finalidad de prevenir eventuales represalias.

En primer término, la confidencialidad se proyecta en un requisito esencial, pues garantiza la protección de los datos aportados por los denunciantes conforme a los procedimientos de queja interna. Esta salvaguarda adquiere particular relevancia en supuestos de acoso sexual o en relación con infracciones de especial gravedad, y, al menos en un primer análisis, contribuye a la creación de un entorno que alienta la comunicación de irregularidades sin temor a consecuencias adversas. No obstante, este enfoque puede generar dificultades cuando el denunciado solicita acceso a la información que considera que le concierne, ya que se ve limitado en su capacidad para acceder a información de forma trasparente y adecuada. Aquí surge una clara necesidad de balance entre los derechos de los implicados, conforme se observa en el caso en análisis y que la juzgadora lo ha resuelto.

Ante esta situación, el solicitante de acceso (denunciado) ha optado por activar la acción de habeas data como una forma para exigir la transparencia en el proceso organizacional Whistleblowing. No obstante, el habeas data, si bien permite el acceso a los datos de carácter personal, no siempre se revela como el mecanismo más idóneo cuando el propósito del solicitante

es determinar los elementos de prueba relevantes en contextos donde se imponen acusaciones de gravedad, pues su diseño antecedente se orienta a la protección de la autodeterminación informativa más que a la habilitación de estrategias defensivas frente a un proceso penal.

En consecuencia, la Corte Constitucional, a través del voto salvado del magistrado Jhoel Escudero Solíz, formula la guía que niega la admisibilidad del recurso en supuestos específicos en los que se pretende el acceso a datos que conciernen al propio solicitante, siempre que estos se encuentren suscritos en el texto de una denuncia. La argumentación sostiene que la denuncia es, por su naturaleza, un documento que agrupa no solo información personal sino también otros elementos fácticos que, aun al vincularse a la persona del solicitante, no alcanzan la condición de datos personales en sentido estricto, puesto que aluden a conductas o contextos que el ordenamiento no cataloga como información protegida. Esta posición se refuerza particularmente cuando el solicitante argumenta que se ha vulnerado su derecho a la defensa, como ocurre en el caso en análisis (Sentencia: No. 47-19-JD/22, 2022).

Con respecto a este tema, los entrevistados exponen dos criterios, por un lado, la acción de habeas data es una garantía constitucional efectiva para asegurar el acceso a información personal, incluyendo información sobre los detalles relacionados con el momento, el lugar y la forma (tiempo, lugar y modo) en que ocurrieron los hechos denunciados. Por otro lado, conforme a lo expuesto por la Corte Constitucional, se ha indicado que, a efectos de obtener la información completa relativa a los supuestos hechos que sustentan una denuncia, la acción de protección se revela como el mecanismo más idóneo (Sentencia: No. 47-19-JD/22, 2022). Esta conclusión se basa en que los correspondientes expedientes no únicamente contienen información de carácter personal, sino que, a su vez, se vinculan de manera inmediata con datos esenciales para el correcto ejercicio de derechos procesales, tales como el debido proceso y el derecho de defensa.

La Constitución del Ecuador (2008), al establecer que el habeas data, tiene como propósito principal amparar el derecho del accionante a la protección de sus datos personales, mediante el ejercicio del principio de autodeterminación informativa, ha permitido que la jueza resuelva y aplique el artículo 92 de la mencionada norma, de esta manera equilibra los derechos en el sentido de velar por el acceso y conocimiento de los datos personales del titular solicitante, pero a la vez, respetando los derechos de protección de datos de terceros involucrados en el proceso Whistleblowing, al hacerlo, respeta los principios constitucionales acerca de acceso a la información y confidencialidad, de este modo, se reconoció al titular el derecho a conocer todos los aspectos vínculados con la administración y manipulación de sus datos, y, de ser procedente, a solicitar su rectificación o anulación. No obstante, la resolución también destaca la importancia de continuar desarrollando la norma, ya que algunos casos pueden plantear situaciones complejas que no están completamente cubiertas por los criterios actuales.

En definitiva, la resolución de la jueza en el caso habeas data (N° 17230-2018-19732, 2019) aborda los principios establecidos en la Constitución y la normativa que pueda ser aplicada a la acción, enmarca un balance adecuado entre el acceso a la información personal y la protección de los derechos de confidencialidad de terceros mediante la adopción del principio de disociación, es decir encuentra una solución intermedia sin desviarse del propósito de la acción, se centra exclusivamente en el objeto del habeas data debido a que es la acción que se está planteando, en este sentido, se acopla al planteamiento de la doctrina que establece una solución mediante la aplicación del principio de disociación de datos, con el fin de evitar el acceso indebido a información de terceros, que según el autor Ticli (2021) permitiría la permanencia de la confidencialidad de los datos.

En este sentido, la jueza del caso en análisis se enfocó ajustando la realidad con las normas y las reglas establecidas por la Corte, evitando la desnaturalización al ordenar la entrega de información referente al sujeto activo de la acción, siguiendo los lineamientos establecidos por el órgano constitucional para proteger los derechos involucrados en el proceso permitiendo la protección igualitaria a las partes. Este caso refleja una problemática recurrente en acciones de habeas data, especialmente cuando se intenta utilizar esta herramienta como un medio para otras finalidades, como la defensa en donde los datos solicitados pueden relacionarse con el sujeto, pero no necesariamente lo pueden identificar.

Sobre aquellos datos susceptibles para acceder de forma personal, el máximo órgano constitucional en su análisis del caso de habeas data (N° 17230-2018-19732, 2019), ha establecido nuevas reglas para estos casos, las cuales se centran en identificar específicamente los datos personales dentro de los contextos de denuncias, la Corte analiza la pretensión del accionante en el caso analizado y determina que la información sobre el "tiempo, lugar y modo" en que ocurrieron los acontecimientos no corresponde a la categoría de datos personales, dado que no permiten la identificación ni hacen posible identificar a un sujeto, más bien esta información se refiriere exclusivamente a hechos, lo que no constituye dato personal (Sentencia: No. 47-19-JD/22, 2022). Este cambio de criterio no solo crea un precedente relevante, sino que también introduce lineamientos que podrán aplicarse en futuros casos, especialmente en contextos relacionados con protocolos de Whistleblowing, aportando claridad en la delimitación de los datos personales y su acceso.

3.4. Conclusiones

- El análisis teórico y normativo demuestra que el Ecuador cuenta con un marco jurídico adecuado para la protección de datos personales y el acceso a la información personal,

consolidado a través de la Constitución, la Ley Orgánica de Protección de Datos Personales y la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. No obstante, dicho marco legal carece de una normativa particular que trate de manera integral los protocolos de Whistleblowing, esta omisión normativa genera vacíos que dificultan la armonización entre los derechos a la confidencialidad del denunciante y al acceso del denunciado a su información personal, afectando la eficacia de la protección de derechos en contextos de denuncia interna donde confluyen derechos de igual jerarquía.

- El análisis del caso No. 17230-2018-19732 evidencia que la activación de la acción de habeas data permite de forma efectiva el acceso a datos personales del accionante, sin vulnerar la confidencialidad del denunciante, mediante la aplicación correcta de principios de transparencia y disociación, delimitando la entrega de información estrictamente personal y excluyendo los datos que pudieran revelar la identidad del denunciante, esta solución judicial representa un precedente valioso que confirma la posibilidad de armonizar derechos en tensión cuando a falta de norma se aplican principios. A pesar de esto, se ha evidenciado que el caso en cuestión ha impulsado a la organización CNR a flexibilizarse parcialmente ante las solicitudes de acceso a la información personal en el contexto de los protocolos de denuncia Whistleblowing. No obstante, persisten dificultades para que los denunciantes accedan de manera adecuada a su información, conforme establece los parámetros legales establecidos en la normativa nacional.
- La jurisprudencia constitucional, en especial la Sentencia 47-19-JD/22, ha sido determinante para precisar el contenido y alcance del derecho de acceso a la información personal en contextos donde intervienen terceros, especialmente en el caso analizado, se ha establecido que los datos personales no se limitan a nombres o identificadores directos,

sino que incluyen información relacionada con el entorno laboral, familiar o circunstancial del titular que permita hacerlo identificable y que pueda afectar la dignidad del titular, este efecto evolutivo dota de mayor claridad a los operadores de justicia para una correcta aplicación de las normas y que la creación de reglas jurisprudenciales que abarcan la amplitud de la protección en los contextos Whistleblowing servirán de guía en casos futuros con características y complejidades similares, de esta manera se resalta la importancia de una jurisprudencia que se adapta a las realidades cambiantes y que proporciona un marco de referencia para la toma de decisiones judiciales a futuro.

- Si bien la acción de habeas data es idónea para permitir el acceso a los datos personales propios en contextos de protocolos Whistleblowing, no siempre es el mecanismo más eficaz cuando el objetivo principal es ejercer el derecho a la defensa. En el caso analizado, se constató que la pretensión del accionante tenía una finalidad más amplia: obtener elementos probatorios para su defensa, lo que excede el marco de protección del habeas data. En tales casos, la acción más adecuada sería la acción de protección, por cuanto permite discutir violaciones más amplias de derechos.
- En términos generales, se concluye que las medidas normativas y jurisprudenciales analizadas han sido eficaces para garantizar el derecho al acceso a la información personal en el marco de los protocolos Whistleblowing, es decir que la acción de habeas data ha demostrado utilidad como un medio de acceso y protección, siempre que se apliquen adecuadamente los principios de disociación, proporcionalidad y pertinencia como un punto de equilibrio entre estos derechos. Sin embargo, este balance depende en gran medida del criterio judicial, por lo que su aplicación no es plenamente previsible ni uniforme en ausencia de una regulación legal específica sobre Whistleblowing.

Finalmente, el habeas data analizado, también ha permitido que los abogados y las personas denunciadas en el contexto de los protocolos de Whistleblowing puedan conocer que mediante la activación de esta garantía jurisdiccional es posible acceder, conocer y en consecuencia proteger sus datos personales en sentido estricto y amplio.

3.5. Recomendaciones

- Es esencial la creación de una ley específica sobre los mecanismos de denuncia interna Whistleblowing que regule los derechos y obligaciones de todos los actores implicados en estos protocolos, la cual deberá tener la intervención técnica de la Defensoría del Pueblo y el Superintendente de Protección de Datos Personales, estableciendo canales para garantizar los derechos del debido proceso, el acceso a la información y protección de datos personales, esto permitirá armonizar el principio de confidencialidad con el derecho de defensa y la protección de datos personales de los titulares, además esta ley permitiría cerrar lagunas legales, mediante la codificación de principios rectores, obligaciones institucionales, garantías mínimas para el denunciante y el denunciado, y mecanismos concretos de protección.
- Las organizaciones deberían desarrollar directrices claras en una guía de carácter técnico y operativo interno en sus instituciones para la correcta gestión de los protocolos de denuncia interna, estableciendo una adecuada gestión de datos personales, que incluya protocolos de seguridad, capacitación continua del personal, determinando los procedimientos a fin de procurar el debido respeto de los derechos. Estas medidas serán fundamentales y adecuadas para prevenir litigios y proteger la información de los involucrados con respecto al tratamiento y acceso a información personal, especialmente en situaciones donde las

denuncias no ingresan en el ámbito judicial y permanezcan dentro de estas instituciones, esto con la finalidad de evitar vulneraciones al derecho de protección de datos personales.

- De la misma forma, todas las entidades que manejan los protocolos Whistleblowing, en su calidad de entes protectores de los derechos de los denunciantes, deberían establecer dentro de sus disposiciones internas la adopción de lineamientos y mecanismos de actuación que promuevan la judicialización de casos graves derivados de denuncias internas, estas acciones garantizarán el acceso efectivo al derecho a la defensa y evitará la afectación de su derecho al honor por parte del denunciado.
- La autoridad de protección de datos personales, como órgano rector técnico, debería emitir un documento informativo para todas los organismos estatales y no estatales en el tratamiento de datos personales, con mayor énfasis a instituciones que manejen datos en contextos de investigación disciplinaria interna, en el que se indique claramente qué constituye un dato personal o información personal en sentido estricto y amplio, conforme lo ha manifestado la Corte Constitucional mediante la estructuración de sus reglas jurisprudenciales. Este instrumento deberá establecer métodos puntuales para el tratamiento de datos en los contextos Whistleblowing, promoviendo una aplicación uniforme en las instituciones lo que permitiría establecer un marco operativo coherente con la Ley Orgánica de Protección de Datos Personales y con los estándares jurisprudenciales de la Corte Constitucional.
- Los expertos del derecho deben realizar un análisis integral de las directrices emanadas tanto por la legislación vigente como por la jurisprudencia, con el objetivo de actuar conforme a derecho en relación con la naturaleza y pretensión de la garantía jurisdiccional, este enfoque permitirá una aplicación adecuada y efectiva de los mecanismos legales

establecidos para la protección de los derechos en relación a los datos personales aplicando la supresión para contrarrestar afectaciones a la dignidad de los denunciados en el proceso seguido contra ellos.

- La academia mediante la carrera profesional del derecho debe actualizar sus mallas curriculares, igualmente la escuela de formación judicial del Consejo de la Judicatura, debería incorporar módulos sobre jurisprudencia constitucional aplicada a los derechos de protección de datos personales incluyendo en los espacios digitales, especialmente en torno al habeas data vinculada con el Whistleblowing, desarrollando programas de formación continua obligatorios para operadores jurídicos, esta acción, liderada por el Consejo de la Judicatura y las universidades acreditadas, asegurará que los criterios jurisprudenciales se integren en la práctica profesional y que los operadores jurídicos puedan invocar adecuadamente las garantías constitucionales disponibles en la ley.

BIBLIOGRAFÍA

Alzate Peralta, L. A., Freire Gaibor, E. F., & Martínez Pérez, O. (2024). Desafíos del habeas data en la protección de datos personales en el ordenamiento jurídico ecuatoriano. *European Public & Social Innovation Review*, *9*, 1–21. https://doi.org/10.31637/EPSIR-2024-1842

Andía, M. G., & Colombato, I. (2021). Tensiones entre el derecho al acceso a la información y la protección de datos personales en la vacunación contra el COVID-19 en Argentina. *Millcayac-Revista Digital de Ciencias Sociales*, *8*(15), 29–34. https://revistas.uncu.edu.ar/ojs/index.php/millca-digital/article/view/4823

Asamblea General de la ONU. (1990). *PRINCIPIOS RECTORES PARA LA REGLAMENTACIÓN DE LOS FICHEROS COMPUTADORIZADOS DE DATOS PERSONALES*. ORDEN JURÍDICO NACIONAL. https://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf

Ayala Endara, O. A., Calle Burgos, K. P., & Carrera García, V. F. (2024). La necesidad de uniformidad en las Jurisprudencias Erga Omnes en Ecuador: Análisis doctrinal y consecuencias jurídicas. *DERECHO CRÍTICO:REVISTA JURÍDICA, CIENCIAS SOCIALES Y POLÍTICAS*, *5*, 1–24. https://doi.org/https://doi.org/10.53591/dcjcsp.v5i5.599

Ballesteros Sánchez, J. (2020). Pautas y recomendaciones técnico-jurídicas para la configuración de un canal de denuncias eficaz en organizaciones públicas y privadas. La perspectiva española. *Derecho PUCP*, *85*, 41–78. https://doi.org/10.18800/DERECHOPUCP.202002.002

Barreiro, D. A. (2024). La necesaria figura del alertador (whistleblower) en el ámbito legal latinoamericano. *Encuentros Multidisciplinares*, *26*, 3–3. http://www.encuentros-multidisciplinares.org/revista-77/daniel-amoedo.pdf

Barrio, A. (2022). La regulación del derecho a la protección de datos en los Estados Unidos: *CUADERNOS DE DERECHO TRANSNACIONAL*, *14*(2), 186–193. https://doi.org/10.20318/CDT.2022.7181

Bazán, V. (2005). El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado. *Estudios Constitucionales: Revista Del Centro de Estudios Constitucionales, ISSN 0718-0195, ISSN-e 0718-5200, Año 3, Nº. 2, 2005, Págs. 85-139*, *3*(2), 85–139. https://dialnet.unirioja.es/servlet/articulo?codigo=2034014

Bernal-Camargo, D. R., & Gómez-Córdoba, A. I. (2022). El derecho a la protección de datos personales en la investigación biomédica en Colombia: Una mirada desde el soft law y el hard law. *Revista Chilena de Derecho y Tecnología*, *11*(1), 361–396. https://doi.org/10.5354/0719-2584.2022.66319

Bonilla Gutiérrez, J. C. (2024). IA y Privacidad: Protegiendo la Autodeterminación Informativa en la Era Digital. *Revistas.Unam.MxJCB GutiérrezRevista de La Facultad de Derecho de México, 2024•revistas.Unam.Mx*, 127–128. https://doi.org/10.22201/fder.24488933e.2024.290.89719

Bru Cuadrada, E. (2007). La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. *IDP: Revista de Internet, Derecho y Política = Revista d'Internet, Dret i Política, ISSN-e 1699-8154, Nº. 5, 2007*, *5*, 7. https://dialnet.unirioja.es/servlet/articulo?codigo=2372618&info=resumen&idioma=SPA

Buedo, P., Sánchez, L., Ojeda, M. P., Della-Vedova, M. N., Labra, B., Sipitria, R., Centineo Aracil, L., Consentino, S., Varela, I., Yabar Varas, C., Apaza, G., Krasnow, A., Vílchez, S., & Luna, F. (2023). Consentimiento informado y directivas anticipadas: análisis comparado de la legislación en América Latina. *Centro Nacional de Desarrollo e Investigación En Tecnologías Libres (CENDITEL)*, 37–38. https://doi.org/10.1344/RBD2023

Carbonell, M. (2006). *El derecho de acceso a la información como derecho fundamental*. Orfis.Gob.Mx. https://www.orfis.gob.mx/BibliotecaVirtual/archivos/08042016024901.pdf

Castillo Chípuli, A. M. (2024). La protección de denunciantes de actos de corrupción (whistleblowers) en el Sistema Interamericano de Derechos Humanos. El Caso Viteri Ungaretti y Otros vs. Ecuador. In *tirant lo blanch*. TIRANT HUMANIDADES.

Cedeño Cedeño, R. J., Maldonado Palacios, I. A., & Vizcaíno Zúñiga, P. I. (2023). Metodología de la investigación científica: guía práctica. *Ciencia Latina Revista Científica Multidisciplinar*, *7*(4), 1–40. https://doi.org/10.37811/CL_RCM.V7I4.7658

Chana Durán, J. L. (2022). *"Bases jurídicas fundamentales para plantear una futura ley especifica de protección de datos personales en nuestro país"* [Doctoral dissertation-Repositorio Institucional Universidad Mayor de San Andrés]. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=%22Bases+jur%C3%ADdicas+fundamentales+para+plantear+una+futura+ley+especifica+de+protecci%C3%B3n+de+datos+personales+en+nuestro+pa%C3%ADs%22&btnG=

Chipuxi Fajardo, L., & Guaña Moya, J. (2023). Impacto de la inteligencia artificial en la ética y la privacidad de los datos. *RECIAMUC*, *7*(1), 923–930. https://doi.org/10.26820/RECIAMUC/7.(1).ENERO.2023.923-930

Constitución de La República Del Ecuador, 449 Registro Oficial No. 449 , 20 de Octubre 2008.Última Reforma: Tercer Suplemento del Registro Oficial 568, 30-V-2024 25 (2008). www.lexis.com.ec

Cruz Ángeles, J. (2023). Las transferencias de datos a través del Metaverso a la luz de los últimos acuerdos (UE - EE.UU.). El fenómeno "tú a Londres y yo a California." *CUADERNOS DE DERECHO TRANSNACIONAL*, *15*(2), 251–292. https://doi.org/10.20318/CDT.2023.8056

de la Vega Silva, F., & Otero Carreón, J. (2013). *ACERCAMIENTO AL WHISTLEBLOWING*. Pontificia Universidad Católica de Valparaiso. https://www.pucv.cl/uuaa/site/docs/20190619/20190619162259/memoria_2013_felipe_de_la_vega_javiera_otero.pdf

Echeverría Mantilla, V. H. (2013). *Desarrollo de una metodología para la administración integral del riesgo de fraude empresarial basada en el modelo COSO ERM*. Escuela Politécnica Nacional, BIBDIGITAL. https://bibdigital.epn.edu.ec/handle/15000/8071

Espinosa Velarde, C. F. (2017). *Derechoalolvidodigital-Reconocimiento de los criterios de aplicabilidad del derecho al olvido digital en el Ecuador*. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Derechoalolvidodigital-Reconocimiento+de+los+criterios+de+aplicabilidad+del+derecho+al+olvido+digital+en+el+Ecuador&btnG=

Gárate Amoroso, J., Reina Cunín, J., Samaniego Nugra, E., & Loyola Moreano, K. (2021). Habeas Data: origen y evolución. *Revista Lex*, *4*(13), 197–210. https://doi.org/10.33996/REVISTALEX.V4I13.82

Garcés Córdova, F. A., Diaz Basurto, I. J., & Moreno Arvelo, P. M. (2023). Evaluación del derecho al olvido en la salvaguarda de datos personales en Ecuador. *Dilemas Contemporáneos: Educación, Política y Valores*. https://doi.org/10.46377/DILEMAS.V11IESPECIAL.3949

García Roldán, J. E. (2024). *El impacto del RGPD en las políticas y prácticas de protección de datos en Ecuador.* UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABI . https://repositorio.uleam.edu.ec/handle/123456789/6426

Garrido Vidal, R. C. I. (2024). Tratamiento y protección de los datos personales en la ley N° 19.628: historia, evolución, regulación, mecanismos de protección y deficiencias. *PORTAL DE REVISTAS ACADÉMICAS CHILENAS*. https://doi.org/10.58011/7S2D-E131

Guillén Ortega, E. del C. (2021). *La consolidación de los canales de denuncia en el derecho español: el "whistleblower" y su protección*. E-Repositori UPF. https://repositori.upf.edu/items/3919bc77-95bd-43eb-90be-371d9d17c6e0

Laro González, M. E. (2021). PRINCIPIO DE PROPORCIONALIDAD Y TRATAMIENTO DE DATOS PERSONALES EN EL PROCESO PENAL1. In *Departamento de Derecho Procesal (Universidad de Sevilla)*. https://idus.us.es/server/api/core/bitstreams/16dda481-6d6d-456b-8228-1dc6231527b3/content

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. (2009). Registro Oficial Suplemento 52 de 22-Oct-2009. https://www.lexis.com.ec/biblioteca/ley-organica-garantias-jurisdiccionales-control-constitucional

Ley Orgánica de Protección de Datos Personales (2021). https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Ley Orgánica Integral Para Prevenir y Erradicar La Violencia Contra Las Mujeres, Registro Oficial Suplemento 175 de 05-feb.-2018 (2018). https://www.lexis.com.ec/biblioteca/ley-prevenir-erradicar-violencia-contra-mujeres

Ley para Prevenir y Erradicar la Violencia contra las Mujeres. (2018, January 31). Registro Oficial Suplemento 175 de 05-Feb.-2018. https://www.lexis.com.ec/biblioteca/ley-prevenir-erradicar-violencia-contra-mujeres

Lisoni Caro, D. A. (2020). *Proyecto de Ley que regula la protección y el tratamiento de los datos personales y crea la agencia de protección de datos personales: análisis y propuestas a la luz del principio de responsabilidad proactiva*. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Proyecto+de+Ley+que+regula+la+protecci%C3%B3n+y+el+tratamiento+de+los+datos+personales+y+crea+la+agencia+de+protecci%C3%B3n+de+datos+personales%3A+an%C3%A1lisis+y+propuestas+a+la+luz+del+principio+de+responsabilidad+proactiva&btnG=#d=gs_cit&t=1747263341439&u=%2Fscholar%3Fq%3Dinfo%3AmlWr-Zif46gJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Des

Lopera Echavarria, J. D., Ortiz Vanegas, J., Ramírez Gómez, C. A., & Zuluaga Aristazába, M. U. (2010). *EL MÉTODO ANALÍTICO COMO MÉTODO NATURAL*. *1*, 1–28. https://www.redalyc.org/pdf/181/18112179017.pdf

Maqueo Ramírez, M. S., Moreno González, J., & Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho (Valdivia)*, *30*(1), 77–96. https://doi.org/10.4067/S0718-09502017000100004

Mora Rojas, E. J. (2019, October 18). *De la Identidad al Habeas Data*. Centro Nacional de Desarrollo e Investigación En Tecnologías Libres (CENDITEL).

Naciones Unidas. (1948, December 10). *La Declaración Universal de los Derechos Humanos*. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Naciones Unidas. (1966). *Pacto Internacional de Derechos Civiles y Políticos*. https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr_SP.pdf

Nizama Chávez, L. M., & Nizama Valladolid, M. (2020). El enfoque cualitativo en la investigación jurídica, proyecto de investigación cualitativa y seminario de tesis. *Vox Juris, ISSN 1812-6804, Vol. 38, Nº. 2, 2020, Págs. 69-90*, *38*(2), 69–90. https://doi.org/10.24265/voxjuris.2020.v38n2.05

OEA. (1969). *Convención Americana sobre Derechos Humanos (Pacto de San José)*. https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

OEA. (2022). *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales*.

Ormazabal Sánchez, G. (2021). El tratamiento procesal de la información constitutiva de secreto empresarial: especial referencia a las medidas de protección de la confidencialidad de la Ley 1/2019. *InDret: Revista Para El Análisis Del Derecho*, 219–225. https://doi.org/10.31009/InDret.2021.i3.08

Pérez Miras, J. (2019, January 11). *El derecho a la protección de datos y a la privacidad: una perspectiva comparada entre la Unión Europea y Estados Unidos.* https://idus.us.es/items/a17fc332-45db-4e0a-a593-431f41c34634

Pérez Rojas, R. O. (2023, August). *Inteligencia artificial aplicada a la ley de protección de datos*. Google Libros; E-Books del Ecuador. https://books.google.com.ec/books?hl=es&lr=&id=WWTjEAAAQBAJ&oi=fnd&pg=PA7&dq=inteligencia+artificial+aplicada+a+la+ley+de+proteccion+de+datos+perez+rojas&ots=88wUbqU8NL&sig=rcRSLbmwujTHD8-xi2KdpoHk-2E&redir_esc=y#v=onepage&q=inteligencia%20artificial%20aplicada%20a%20la%20ley%20de%20proteccion%20de%20datos%20perez%20rojas&f=false

Pino Salazar, V. A., & Quintero Páez, A. A. (n.d.). *ANALISIS DEL PRINCIPIO PRO HOMINE EN LOS TRATADOS INTERNACIONALES DE DERECHOS HUMANOS SUSCRITOS POR COLOMBIA.* Retrieved June 26, 2025, from https://www.researchgate.net/profile/Ashley-Quintero-Paez/publication/371250939_ANALISIS_DEL_PRINCIPIO_PRO_HOMINE_EN_LOS_TRATADOS_INTERNACIONALES_DE_DERECHOS_HUMANOS_SUSCRITOS_POR_COLOMBIA/links/647a5c02b3dfd73b775dd0a8/ANALISIS-DEL-PRINCIPIO-PRO-HOMINE-EN-LOS-TRATADOS-INTERNACIONALES-DE-DERECHOS-HUMANOS-SUSCRITOS-POR-COLOMBIA.pdf

Polo Roca, A. (2020). El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado. *Revista de Derecho Político*, *108*, 180. https://doi.org/10.5944/RDP.108.2020.27998

Porcelli, A. M. (2019). La Protección de los Datos Personales en el Entorno Digital. Los Estándares de Protección de Datos en los Países Iberoamericanos. *REVISTA QUAESTIO IURIS*, *12*(2), 465–497. https://doi.org/10.12957/RQI.2019.40175

Quiroz Papa de García, R. (2016). El Hábeas Data, protección al derecho a la información ya la autodeterminación informativa. *Scielo.Org.Pe*, 23–44. http://www.scielo.org.pe/scielo.php?pid=S2071-50722016000200002&script=sci_abstract

Reglamento Para La Recepción y Trámite de Denuncias Para Investigación Administrativa En La Contraloría General Del Estado, Acuerdo de la Contraloría General del Estado 34 Registro Oficial Suplemento 50 de 20-oct-2009 (2009). https://www.oas.org/juridico/pdfs/mesicic4_ecu_regCGE.pdf

Rovira Jurado, Z. E., Robles Riera, L. E., & Castillo Méndez, J. A. (2023). Protección de datos en el contexto de la promulgación de la Ley Orgánica de Protección de Datos Personales en Ecuador. *Polo Del Conocimiento*, *8*(8), 1355–1373. https://doi.org/10.23857/pc.v8i8.5908

Sánchez Lay, F. S. (2010). *La protección de denuncias de hechos de corrupción: la regulación del whistleblowing en el derecho comparado*. Repositorio Académico de La Universidad de Chile; Universidad de Chile. https://repositorio.uchile.cl/handle/2250/107121

Sentencia 001-14-PJO-CC, Corte Constitucional del Ecuador (2014). https://vlex.ec/vid/jurisprudencia-vinculante-presentada-524639466

Sentencia 182-15-SEP-CC, 607-Segundo Suplemento (2015). https://vlex.ec/vid/aceptese-accion-extraordinaria-proteccion-645092269

Sentencia N° 17230-2018-19732, Unidad Judicial Civil del Distrito Metropolitano de Quito, Proceso N° 17230-2018-19732 (2019). https://procesosjudiciales.funcionjudicial.gob.ec/actuaciones

Sentencia: No. 47-19-JD/22, Edición Constitucional Nº 190 - Registro Oficial (2022). https://vlex.ec/vid/47-19-jd-22-924636391

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

Ticli Vocos, C. M. (2021, June 29). *Derecho de acceso a la información pública: Nota a fallo "Sindicato Unión Obreros y Empleados Municipales (SUOEM) y Otro c/ Municipalidad de Córdoba – Amparo – Acción De Habeas Data Colectivo" (Expte. N° 6411412), dictado por la Cámara en lo Contencioso Administrativo de Segunda Nominación de la ciudad de Córdoba*. Universidad Siglo 21. https://repositorio.21.edu.ar/server/api/core/bitstreams/f4ed3819-4314-4315-aa01-102905355ccc/content

Zaror Miralles, D. (2019). Implementación de un modelo de autorregulación voluntaria en materia de protección de datos personales. *Revista de Derecho Aplicado LLM UC*, *3*(3), 1–19. https://doi.org/10.7764/RDA.0.3.1069