Propuesta de modificación al instructivo ISCPS007 “Servicios de Seguridad Electrónica” para el adecuado tratamiento y suministro de grabaciones de videovigilancia como prueba licita, en el marco de los procesos disciplinarios adelantados al interior de la Electrificadora de Santander S.A. E.S.P.

Nicole Barrera Vásquez

Trabajo de grado para optar por título de abogada

Directora

Ana Patricia Pabón Mantilla

Doctora en Derecho e Investigadora Senior

Tutor

Lida Mayerly López Pedraza

Especialista en Derecho Laboral y Relaciones Industriales

Universidad Industrial de Santander

Facultad de Ciencias Humanas

Escuela de Derecho y Ciencia Política

Bucaramanga

2024

Dedicatoria

A mi abuela Ana Flor Sierra, que desde mis primeros años de vida vio en mi un potencial para ser “una mujer de leyes y gobierno”; Guardé en mi corazón sus palabras y heme aquí.

Agradecimientos

Primeramente, a Dios por dotarme de sabiduría y constantemente abrir caminos llenos de bendiciones en mi vida.

A mi familia, mis padres Edwin Barrera y Angélica Vásquez quienes, pese a las adversidades, se esforzaron por brindarme constantemente el acceso a una educación de calidad; por amarme, respetarme e inculcarme todos los valores que me caracterizan hoy en día; soy enormemente privilegiada de que sean mis padres.

A mi hermano Sebastián Barrera, por sacarme siempre una sonrisa y hacerme olvidar un rato de las preocupaciones de la vida. A mi primo Daniel Barrera, que ha sido en estos últimos años mi fiel amigo, mi hermano y mi confidente, gracias por ser mi soporte emocional.

A mi mejor amigo Andrés Hernández, por ser mi compañero de clases durante cinco lindos años, por escucharme, apoyarme y compartir conmigo buenos y malos momentos; eres el mayor regalo que me dejó la UIS, no sé si podría haberlo logrado sin ti.

A mis colegas y amigos Valentina Franco, Sebastián Flórez y Jose Álvarez, gracias por haber hecho de mi vida universitaria una colección de agradables recuerdos y contribuir en mi formación personal y profesional.

Al cuerpo de docentes y administrativos de la Escuela de Derecho de la Universidad Industrial de Santander UIS, por forjar mi carácter como persona e instruirme en la academia como profesional, por enseñarme a tener pensamiento crítico e inculcarme la función social del abogado al servicio del pueblo. A las profesoras Marely Cely Silva y Angy Maryuri Bernal, por haberme trasmitido su pasión y amor por el Derecho Laboral a través de sus

enseñanzas en el aula de clases y Consultorio Jurídico. A la profesora e investigadora Ana Patricia Pabón, por haber dirigido este trabajo de manera muy atenta y excepcional.

Finalmente, a la Electrificadora de Santander S.A. E.S.P., empresa en la que tuve la oportunidad de realizar mi práctica profesional, en especial a mis colegas y amigos, los abogados John Jairo Hurtado, Berta Juliana Cala, Luz Dary Quintero, Claudia Johanna Olarte, quienes me recibieron de brazos abiertos y me hicieron parte de su hermosa familia de ALSEG en los seis meses que pude estar junto a ellos. A Luz Helena Díaz, quien antes que ser mi jefe, fue una persona humilde, bondadosa y de gran corazón. Finalmente, a Lida Mayerly López, abogada laboralista a quien admiro y que fue mi tutora en el curso de este proyecto.

Gracias a todos por convertir la Universidad en una de las etapas más preciadas de mi vida, los llevo en mi alma.

Tabla de Contenido

Pág.

Lista de figuras

Resumen

Título: Propuesta de modificación al instructivo ISCPS007 “Servicios de Seguridad Electrónica” para el adecuado tratamiento y suministro de grabaciones de videovigilancia como prueba licita, en el marco de los procesos disciplinarios adelantados al interior de La Electrificadora de Santander S.A. E.S.P.[1]

Autor: Nicole Barrera Vásquez[2]

Palabras clave: Habeas data, derecho a la intimidad, sistemas de videovigilancia, datos sensibles, tratamiento de datos

Descripción: La práctica adelantada buscó diagnosticar las necesidades de regulación en materia de aplicación de procesos disciplinarios laborales adelantados al interior de la Electrificadora de Santander S.A. E.S.P., en aquellos casos en que se pudiera presentar una tensión de derechos frente a la entrega de material de audio y video. Como resultado de dicho estudio preliminar se determinó la necesidad de creación un nuevo acápite en el instructivo ISCPS007 “Servicios de Seguridad Electrónica” de la Electrificadora de Santander S.A. E.S.P. Dicho instructivo aborda, entre otros temas, las políticas de acceso y suministro de grabaciones captadas por el sistema de videovigilancia (CCTV) de la empresa, las cuales han generado preocupaciones debido a la ausencia de un protocolo claro para la obtención de copias de estas grabaciones por parte de los trabajadores, en los que se garantice la protección de sus derechos. En la actualidad, no existe una normativa explícita que establezca las condiciones, procedimientos y restricciones bajo las cuales estas grabaciones pueden ser entregadas o utilizadas en procesos disciplinarios laborales, lo que representa un riesgo potencial para los derechos fundamentales de los empleados, particularmente el derecho a la intimidad y el derecho al habeas data.

Este trabajo propone una alternativa de solución que se construye mediante una revisión sistemática de las leyes y regulaciones vigentes en materia de tratamiento de datos sensibles, garantizando un equilibrio entre la necesidad de mantener la seguridad en el entorno laboral y la protección de los derechos de los trabajadores. De esta forma, se contribuyó a la creación de un protocolo claro, justo y respetuoso con los principios de confidencialidad y privacidad de los empleados de ESSA.

[1] Trabajo de grado
[2] Facultad de Ciencias Humanas. Escuela de Derecho y Ciencias Políticas. Director Ana Patricia Pabón Mantilla

Abstract

Title: Proposed amendment to the “Electronic Security Services” instructive ISCPS007 for the proper handling and provision of video surveillance recordings as lawful proof, within the framework of the labor disciplinary processes carried out within the Electrificadora de Santander S.A. E.S.P.[3]

Author: Nicole Barrera Vasquez[4]

Keywords: Habeas data, right to privacy, video surveillance systems, sensitive data, data processing.

Description: This thesis project focuses on the proposal to create a new section within the "Electronic Security Services" guidelines of the Electrificadora de Santander S.A. E.S.P. These guidelines address, among other matters, the policies governing access to and the provision of CCTV (closed-circuit television) surveillance recordings by the company's employees. Currently, there is no explicit protocol concerning the conditions, procedures, or restrictions under which copies of these recordings may be provided or used in workplace disciplinary processes, which presents a potential risk to employees' fundamental rights, particularly their right to privacy and their right to habeas data.

The aim of this project is to fill that regulatory gap through a comprehensive investigation into the current laws and regulations concerning the handling of sensitive data, ensuring a balance between the need to maintain security in the workplace and the protection of employees' rights. In doing so, this research will contribute to the development of a clear, fair, and respectful protocol that upholds the principles of confidentiality and privacy for ESSA’s employees, thereby providing a lawful and transparent framework for managing surveillance data.

[3] Bachelor Thesis
[4] Facultad de Ciencias Humanas. Escuela de Derecho y Ciencias Políticas. Director Ana Patricia Pabón Mantilla

Introducción

En los años noventa el Estado colombiano hizo parte de los países pioneros en Latinoamérica en la regulación de la protección de datos. La primera referencia que se encuentra a este tema, surge a partir la creación de la constitución de 1991, donde se incorporan novedosos derechos que no se encontraban previstos en la anterior constitución de 1886, como los derechos a la intimidad y el habeas data, buscando con ello responder a los avances del momento en el marco de globalización y el auge de nuevas tecnologías de la información y la comunicación, cuyo desarrollo daba lugar a situaciones en que la posibilidad de recoger información sensible por muchos medios y su uso podía colisionar con algunos derechos fundamentales.

Acatando los direccionamientos de la OCDE - Organización para la Cooperación y el Desarrollo Económico -, así como los llamados de la Corte Constitucional de legislar al respecto, el Congreso de Colombia expidió en 2008 la primera ley por medio de la cual se reglamentó el Hábeas Data para las personas naturales y jurídicas en relación con los datos referidos a asuntos económicos y financieros, siendo esta, la ley 1266 de 2008. Más adelante, se expide la ley 1581 de 2012, que se centró en regular la protección de datos personales, como factor diferenciador de la anterior ley.

A partir de esta regulación jurídica, se impuso la obligación a entidades y empresas públicas y privadas en el territorio nacional que hagan recolección y manejo de datos, el deber de realizar un adecuado tratamiento, con el fin de evitar los perjuicios que se pueden generar de su inadecuado uso y disposición, así como sanciones derivadas del manejo inapropiado de los mismos. En este sentido, también se han dispuesto de herramientas para dotar a personas naturales y jurídicas de mecanismos para asegurar este derecho en caso de encontrarlo vulnerado, bien sea mediante procesos de carácter civil, penal, disciplinario o sanciones por parte de la Superintendencia de Industria y Comercio, este último teniendo un papel fundamental, como entidad que entre sus funciones tiene la de velar por el cumplimiento de las políticas y garantías de protección de datos.

Aun con una variedad considerable de leyes, decretos y jurisprudencia al respecto, al día de hoy, no se han definido lineamentos explícitos para el suministro de datos por parte de empresas y entidades, en especial cuando se habla de los datos contenidos en sistemas de video vigilancia, y que se requieran para ser utilizados como prueba licita en trámites administrativos de diverso tipo, siendo uno de ellos y el que atiende al caso en particular, el del proceso disciplinario laboral, situación que puede generar un choque entre derechos fundamentales, dado que al no mediar una autorización judicial, se puede ver comprometido el derecho al habeas data y la intimidad de terceros si no se cuenta con autorización de los mismos para que se disponga de las grabaciones y el material sensible.

Partiendo de ese contexto, y con el fin de contribuir con el mejoramiento de procesos al interior de la Electrificadora de Santander S.A. E.S.P. se adelantó un diagnosticó de las necesidades de regulación en materia de aplicación de procesos disciplinarios laborales adelantados al interior de la empresa, con el fin de establecer qué procedimientos y garantías se debían incorporar en los procesos adelantados en la entidad cuando se dispusiera de videos y grabaciones en los que la imagen de los trabajadores fuese capturada. Como resultado de dicho estudio preliminar se determinó la necesidad de creación de un nuevo acápite en el instructivo ISCPS007 “Servicios de Seguridad Electrónica” de la Electrificadora de Santander S.A. E.S.P. Dicho instructivo aborda, entre otros temas, las políticas de acceso y suministro de grabaciones captadas por el sistema de videovigilancia (CCTV) de la empresa, las cuales han generado preocupaciones debido a la ausencia de un protocolo claro para la obtención de copias de estas grabaciones por parte de los trabajadores e inclusive el ente disciplinario, en los que se garantice la protección de sus derechos.

A continuación, se explicará el horizonte metodológico, para luego dar paso a las actividades realizadas en la práctica con la finalidad de responder a la necesidad identificada. Finalmente se proponen unas conclusiones en la que se contrasta el problema determinado con la experiencia y resultados obtenidos.

1. Delimitación del trabajo

1.1.Planteamiento del problema

ESSA al momento de iniciar investigaciones disciplinarias en contra de sus trabajadores, motivadas por faltas cometidas en las instalaciones o con ocasión a sus funciones, inicia los procesos disciplinarios en muchos casos valiéndose de los datos recogidos en los sistemas de videovigilancia, ya que las conductas que se denuncian suelen quedar grabadas. A estas grabaciones se le permite al trabajador tener acceso, previo a la firma de un acuerdo de confidencialidad.

Sin embargo, en estos eventos los trabajadores disciplinados argumentando su derecho a la defensa y contradicción, en consonancia con el derecho fundamental al debido proceso, solicitan copia de las grabaciones, encontrando como respuesta del área encargada que no es viable suministrar esas grabaciones, por tratarse de datos de carácter sensible en donde se puede ver comprometido el derecho a la intimidad de terceros al no tener autorización para su uso y suministro, teniendo en cuenta que se suele tratar de espacios semiprivados, al ser oficinas en donde concurren muchas más personas.

Esta problemática no solo se ha presentado con personal que está siendo investigado, sino que inclusive esta prohibición afecta también a víctimas o quejosos, que desean denunciar un hecho en el que se han visto lesionados, queriendo usar como prueba fundamental para realizar la queja, la grabación que reposa en los sistemas de Videovigilancia.

ESSA como empresa que busca escuchar a sus trabajadores y la practicante de la mano con la profesional Lida Mayerly López Pedraza, ambas pertenecientes al Área de Asuntos Legales y Secretaría General, que es la encargada de brindar todo el apoyo jurídico y acompañamiento en los tramites disciplinarios de la empresa que se llevan a cargo del Área de Servicios Corporativos al interior del equipo de trabajo Administración de Personal, se han planteado la posibilidad de brindar no solo el acceso, sino también, suministrar copia de las grabaciones contenidas en el sistema de video vigilancia CCTV, únicamente con fines de su uso como evidencia en el marco de procesos disciplinarios, en los que los titulares de los

datos se encuentren inmersos, independientemente de si media o no el consentimiento de los demás trabajadores que pudieran concurrir a su alrededor en la circunstancia de espacio/ tiempo en la que estuviese sucediendo una conducta que pudiera contravenir a lo dispuesto en el reglamento interno de trabajo RIT, normas directrices, lineamientos internos, entre otros.

De esta manera, tras una revisión de los manuales de procedimientos de la empresa, específicamente al *Manual de Seguridad Física y Vigilancia*, que para el protocolo de consulta y entrega de material audiovisual del CCTV a trabajadores ESSA, indica que cuando se requiera la consulta de videos o fotografías que reposen en el sistema, deberá procederse según lo dispuesto en el punto *5.3.2 Suministros de videos y/o fotografías a terceros* del instructivo ISCPS007 *Servicios de Seguridad Electrónica.*

Al revisar el punto referido en el párrafo anterior, se encontró que no existía ninguna mención al suministro de videos o fotografías con el objetivo de que puedan ser usadas en tramites disciplinarios, y que la disposición que se encuentra expresa ante las problemáticas actuales de la empresa, ha resultado insuficiente para responder a ellas, siendo esta una gran preocupación entre los administrativos de la empresa al no contar con regulación alguna de este procedimiento.

1.2. Formulación del problema

Con base en lo expuesto, se plantea en el escenario de la práctica empresarial como modalidad de grado para la obtención del título de abogada, la pregunta problema:

¿Qué modificaciones se deben hacer al instructivo ISCPS007 “*Servicios de Seguridad Electrónica”* para el adecuado tratamiento y suministro de datos de carácter sensible, tales como las grabaciones de videovigilancia, en el marco de los procesos disciplinarios adelantados al interior de Electrificadora de Santander S.A. E.S.P.?

1.3.Alcance del Trabajo

La finalidad de esta práctica empresarial consiste en hacer una investigación acción participativa, cuyo producto estará reflejado en un informe final antecedido por tres informes específicos de investigación, en los que se podrá visualizar el estudio y análisis que se hizo para solucionar un problema emergente que aqueja actualmente a ESSA al momento de iniciar investigaciones disciplinarias en contra de sus trabajadores por presuntas conductas cometidas constitutivas de faltas taxativas del Reglamento Interno del Trabajo, en los casos específicos en el que los disciplinados, como titulares de datos, solicitaban el suministro de videos e imágenes de CCTV en los que se visualizaban las presuntas faltas cometidas, datos considerados de carácter sensible por generalmente involucrar la identificación de otras personas trabajadoras.

Así pues, el informe final expondrá la necesidad especifica que tenía ESSA al no contar con una guía o protocolo para el suministro de imágenes y videos a trabajadores que están siendo investigados disciplinariamente o que sean parte procesal en estos, casos en los que se puede ver comprometido y vulnerado el derecho al habeas data, a la intimidad, al debido proceso y contradicción; En este sentido, se elaborará una propuesta de solución a la situación problema, siendo la redacción de un nuevo acápite en el instructivo ISCPS007 de *“Servicios de Seguridad Electrónica”* que se entregará por parte de la practicanta a la empresa para su consideración de uso en casos futuros.

1.4 Objetivos

1.4.1 Objetivo General

Diagnosticar qué modificaciones se deben hacer al instructivo ISCPS007 “*Servicios de Seguridad Electrónica”* para el adecuado tratamiento y suministro de datos de carácter sensible, tales como las grabaciones de videovigilancia, en el marco de los procesos disciplinarios adelantados al interior de Electrificadora de Santander S.A. E.S.P con la

finalidad de sugerir una propuesta de reglamentación que garanticen los derechos a la defensa y contradicción, en consonancia con el derecho fundamental al habeas data e intimidad

1.4.2 Objetivos Específicos

Comprender los elementos doctrinales que existen en torno al debido proceso laboral disciplinario en empresas en Colombia que permitan proponer categorías de análisis sobre la garantía de estos derechos.

Analizar el marco normativo en materia de tratamiento y suministro de datos de carácter sensible, derecho a la intimidad y el habeas data frente al uso de sistemas de videovigilancia en el lugar de trabajo y su uso en procesos disciplinarios laborales.

Evaluar los procedimientos de entrega y suministro de fotos y videos, correspondientes a las grabaciones de las cámaras de seguridad instaladas en las oficinas de la empresa a trabajadores, para su uso exclusivo en trámites disciplinarios laborales, a partir de las categorías de análisis que se derivan de los referentes teóricos y normativos con el fin de proponer una regulación interna.

1.5 Metodología

En el ejercicio del acompañamiento jurídico al área de Asuntos Legales y Secretaría General de ESSA, así como la reunión con personal de otras áreas de la empresa, en especial el área de Servicios Corporativos, encargada de los trámites disciplinarios, se ha identificado previo diagnóstico, una necesidad puntual con respecto a la modificación de los manuales de seguridad física y vigilancia. Para suplir esta necesidad se ha planteado un esquema de realización de la práctica en tres etapas; Se realizará una investigación que buscará nutrirse de información relacionada que se encuentre en el panorama general colombiano, así como la que se pueda obtener de primera mano de la empresa, mediante la constante comunicación y socialización con los profesionales y personal encargado, todo en constante relación con

los actores directos, a saber, y los funcionarios de ESSA. Así pues, se planteará una propuesta de solución que será el producto final de este proyecto.

Primera etapa. La primera etapa de la investigación consistió en identificar cuáles son los elementos que por doctrina, jurisprudencia y ley se han determinado como lineamentos que se deben tener en cuenta a la hora de iniciar procesos laborales de carácter disciplinario al interior de empresas privadas que permitan garantizar el derecho al debido proceso, así como el de defensa y contradicción de las partes involucradas. Estos hallazgos se consignaron en un informe que da cuenta del análisis de las fuentes documentales.

Segunda etapa. La segunda etapa de la investigación consistió en una revisión y análisis sistemático de la regulación que hay en Colombia en materia de tratamiento y suministro de datos en empresas del país, así como el uso de sistemas de video vigilancia en consonancia con la protección del derecho fundamental a la intimidad y el habeas data. Para ello se acudió a la legislación colombiana, Constitución Política, conceptos administrativos, jurisprudencia y consultas con profesionales de EPM (teniendo en cuenta que ESSA es una filial del grupo). Esta etapa permitió configurar un marco de referencia a considerar, nutrido de los elementos doctrinales de la primera etapa, al presentar la solución en la etapa final. El análisis jurídico resultado de la segunda etapa se presentó en el segundo y tercer informe.

Tercera etapa. Tras la finalización de las primeras dos etapas, y a partir de la evaluación de la información obtenida, se propuso la elaboración de un protocolo o “paso a paso”, que pueda ser aplicable para la entrega de material audiovisual que se identifica como de carácter sensible, para fines de uso exclusivo en tramites disciplinarios al interior de la empresa. Este se remitirá para su revisión y visto bueno a la tutora Lida Mayerly López Pedraza; Tras revisión, se presentará propuesta de modificación al instructivo ISCPS007 *“Servicios de Seguridad Electrónica”,* como la inclusión del numeral 5.3.3 de esta guía, a través de la tutora a ESSA quien la compartirá con el área de Servicios Corporativos y el área de Suministro y Soporte Administrativo, quienes serán en ultimas los encargados de adoptar esta nueva reglamentación. Esta nueva reglamentación se podrá encontrar en el informe final.

1.6 Información sobre la empresa

1.6.1 Descripción de la empresa

La Electrificadora de Santander S.A. E.S.P. (ESSA) es una empresa de capital mixto, filial del Grupo empresarial EPM. Dedicada a la prestación de servicios públicos que incluyen generación, distribución, transmisión y comercialización de energía, así como actividades relacionadas y complementarias. ESSA actualmente opera en 87 municipios de Santander, dos del sur Bolívar, cuatro del sur del Cesar y uno de Norte de Santander. Con un amplio catálogo de productos y servicios dirigido tanto a estratos residenciales, así como sectores comercial, industrial y oficial, en modalidad regulada y no regulada. Para desarrollar su objeto social y satisfacer a sus grupos de interés, ESSA ha venido desarrollando, una infraestructura que le faculte cumplir con los estándares de calidad y con las demás normas técnicas y regulatorias establecidas por autoridades competentes. (ESSA, Estatutos Sociales, 2018).

1.6.2 Objeto social

La sociedad tendrá por objeto la prestación del servicio público domiciliario de energía eléctrica y sus actividades complementarias de Generación, Transmisión, Distribución, Comercialización, la Inspección de medidores y sellos de seguridad y la Calibración y ensayos de medidores, patrones, equipos de medida, transformadores e instrumentación eléctrica, así como la prestación de servicios conexos o relacionados con la actividad de servicios públicos, de acuerdo con el marco legal y regulatorio. (ESSA, Estatutos Sociales, 2018).

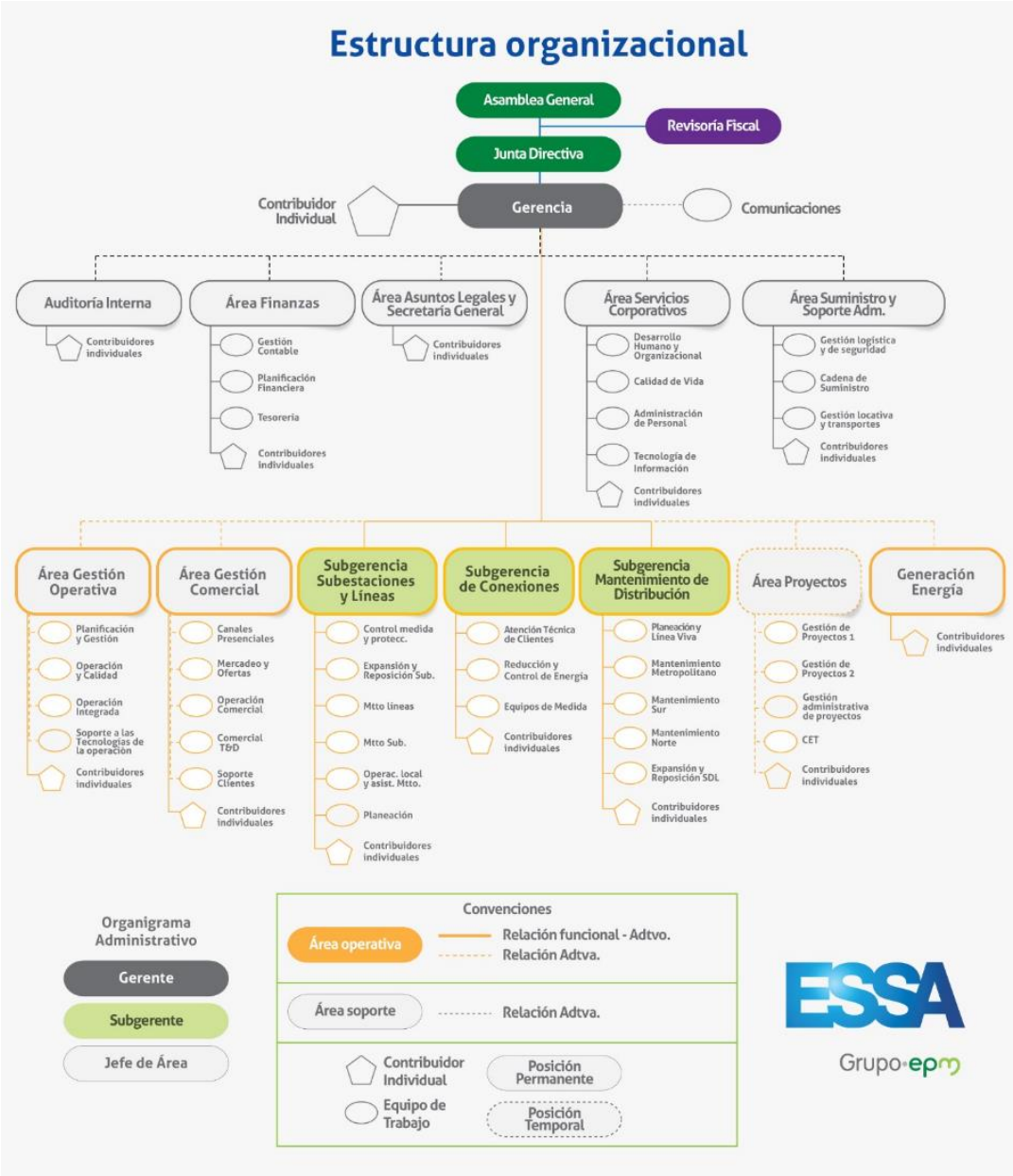
Igualmente para lograr la realización de los fines que persigue la sociedad o que se relacionen con su existencia o funcionamiento, la empresa podrá celebrar y ejecutar cualesquiera actos y contratos, entre otros: prestar servicios de asesoría; consultoría; interventoría; intermediación; importar, exportar, comercializar y vender toda clase de bienes o servicios; recaudo; facturación; toma de lecturas; reparto de

facturas; construir infraestructura; prestar toda clase de servicios técnicos, de administración, operación o mantenimiento de cualquier bien, contratos de leasing o cualquier otro contrato de carácter financiero que se requiera, contratos de riesgo compartido, y demás que resulten necesarios y convenientes para el ejercicio de su objeto social. Lo anterior de conformidad con las leyes vigentes. (ESSA, Estatutos Sociales, 2018).

1.7.Estructura organizacional

Figura 1.

Estructura organizacional ESSA



Nota. Organización de la Electrificadora de Santander S.A E.S.P. Tomado de ESSA (2024). *¿Quiénes somos?* [SITIO WEB]. https://www.essa.com.co/site/informacion-corporativa/quienes-somos.

Figura 2.

Funciones Área de Asuntos Legales y secretaria general

ESSA Grupo epm	ELECTRIFICADORA DE SANTANDER S.A E.S.P.
	FUNCIONES ESTRUCTURA ADMINISTRATIVA ESSA

DEPENDENCIA	EQUIPOS DE TRABAJO	DESCRIPCIÓN (FUNCIÓN BÁSICA)
Gerencia	• Comunicaciones	Liderar, coordinar y controlar la operación de la Organización teniendo en cuenta las estrategias, políticas y lineamientos del Grupo EPM para garantizar el cumplimiento de los indicadores y la consecución de los objetivos económicos, ambientales y sociales que aportan valor a los grupos de interés.
Área Asuntos Legales y Secretaría General		Coordinar y controlar las actividades de consejería legal, gobierno corporativo, proactividad normativa y resolución de disputas y litigios, teniendo en cuenta el marco jurídico aplicable y los lineamientos establecidos por el Núcleo Corporativo del Grupo EPM, para asegurar el cumplimiento legal y la representación de los intereses generales de la organización.

Nota: Funciones estructura administrativa ESSA [SITIO WEB]. https://www.essa.com.co/site/informacion-corporativa/quienes-somos.

1.7.1. Reseña histórica

En 1891, los empresarios Julio Jones y Rinaldo Goelkel introdujeron la energía eléctrica en Santander al construir la primera planta hidroeléctrica en Chitota. Bucaramanga se convirtió así en la segunda ciudad de Colombia en tener este servicio, después de Bogotá, y la primera en suministrar energía a la industria. La empresa de Jones y Goelkel fue la primera en el país en ofrecer luz incandescente para los hogares. (ESSA, sitio web)

En 1927, se fundó la Compañía Penagos S.A., y más tarde se puso en funcionamiento la planta de Zaragoza, que satisfago gran parte de las necesidades energéticas de Bucaramanga. (ESSA, sitio web)

En 1941, se creó la Central Hidroeléctrica del Río Lebrija S.A., la primera empresa del sector eléctrico en Colombia creada por una asociación entre el Estado, el departamento y el municipio. Es así como con fondos estatales y el liderazgo de Benjamín García Cadena, se inició a forjar la historia de Santander. En 1945, se inauguró la primera etapa de la Central Hidroeléctrica del Río Lebrija en Las Palmas, evento tan significativo que el gobernador declaró día cívico ese 24 de abril. Durante esta década se construyeron las centrales de Guepsa y la Cascada en San Gil, así como la línea de transmisión Barrancabermeja, Puerto Wilches y Termobarranca. (ESSA, sitio web)

El 21 de julio de 1975, ESSA se consolidó al incluir la infraestructura existente en García Rovira e Hilebrija Zona Sur, que comprendía la hidroeléctrica La Cómoda, La Empresa de Energía Eléctrica del Socorro y la Cascada de San Gil. Desde entonces, la compañía ha ampliado la cobertura del servicio e incrementado su infraestructura. (ESSA, sitio web)

ESSA apoyó el desarrollo de la Central Hidroeléctrica del Sogamoso, participando en los diseños del proyecto y liderando la empresa promotora hasta que ISAGEN adquirió los derechos de ESSA en los diseños y se comprometió con su construcción. (ESSA, sitio web)

En febrero de 2009, la Nación vendió sus acciones a EPM Inversionistas, lo que permitió a la Gobernación de Santander aumentar su participación accionaria del 14% al 22.48% sin aportar recursos. ESSA se convirtió así, en parte de un grupo empresarial de servicios públicos domiciliarios que opera en varios países. (ESSA, sitio web)

Actualmente, la empresa tiene más de 133 años de historia y celebra su aniversario cada 30 de agosto, promoviendo el progreso y desarrollo del oriente colombiano. (ESSA, sitio web)

Figura 3.

Municipios donde ESSA hace presencia

1.7.2. Misión

Respecto a la misión, la Electrificadora de Santander S.A. E.S.P.: “Busca orientar la gestión corporativa y competitiva del grupo empresarial hacia el logro de sus proyecciones de largo, mediano y corto plazo y su posicionamiento en el sector, unificando las directrices y lineamientos como elementos direccionadores de la organización”. (Grupo EPM, 2023).

1.7.3. Visión

> “En 2025, el Grupo EPM estará creciendo de manera eficiente, sostenible e innovadora; garantizando el acceso a los servicios que preste en los territorios donde esté presente, al 100% de la población; protegiendo a 137 mil nuevas hectáreas de cuencas hídricas, además de las propias, con una operación de carbono neutral y generando $12.6 billones de EBITDA.” (Grupo EPM, 2023).

2. Marcos de referencia

2.1 Marco de antecedentes jurídicos

El marco de antecedentes jurídicos de esta investigación hará un recuento de la normatividad vigente colombiana en materia de Habeas data, derecho a la intimidad, tratamiento y suministro de datos, en especial a aquellos que son titulares de la información y requieren de estos para efecto de uso en procesos administrativos internos, como es el caso del proceso disciplinario laboral.

Inicialmente se encuentra el artículo 15 de la Constitución Política, como el primer antecedente jurídico en materia de hábeas data y protección de datos o derecho a la intimidad.

A su vez, es de vital importancia el artículo 29 del mismo texto, el cual reglamenta el debido proceso como garantía fundamental tanto en trámites judiciales como administrativos.

La relación especial que guardan estos dos artículos tiene que ver con el hecho de, cómo se le puede suministrar al titular de la información imágenes y videos, que comprometen no solo su persona, sino que en la mayoría de ocasiones también la imagen e intimidad de terceros; ello desemboca en un gran problema, cuando estos son requeridos para que el titular pueda hacer efectivo su derecho al debido proceso, y demostrar un supuesto de hecho en aquellas actuaciones procesales que no son de carácter judicial, sino administrativo al interior de empresas, como es el caso concreto.

Al respecto, la ley que vino a reglamentar el tema de la protección y manejo de datos personales es la Ley 1581 de 2012 *“Por la cual se dictan disposiciones generales para la protección de datos personales”*, regulando la forma en que se realizaría el tratamiento de datos personales al interior del territorio colombiano. Son destacables la serie de principios que prevé en el artículo cuarto para su aplicación dirigidos a los responsables y encargados del tratamiento y manejo de bases de datos. Estos son:

a) Principio de legalidad en materia de Tratamiento de datos

b) Principio de finalidad.

c) Principio de libertad.

d) Principio de veracidad o calidad.

e) Principio de transparencia.

f) Principio de acceso y circulación restringida.

g) Principio de seguridad.

h) Principio de confidencialidad. (Ley 1581, 2012, art. 4).

La ley estatutaria también estableció en su artículo octavo un conjunto de derechos para los titulares de los datos personales que sean objeto de tratamiento. Entre estos derechos

se destaca el tener la facultad de poder conocer, actualizar y rectificar sus datos personales ante a los Responsables del Tratamiento o Encargados del Tratamiento, así como obtener la prueba de la autorización de quienes son los responsables del tratamiento (salvo excepción expresa de la ley) e inclusive tener acceso de forma gratuita a los datos que hayan sido objeto de tratamiento. Por otro lado, se menciona que el titular podrá revocar la autorización e incluso solicitar la eliminación del dato cuando determine que en el Tratamiento no se están respetando los principios, derechos, garantías constitucionales y legales, y en consecuencia, presentar quejas por encontrar vulnerados sus derechos de conformidad con lo dispuesto en la ley ante la Superintendencia de Industria y Comercio.

Un aspecto destacable de la ley es el constante énfasis en la importancia de contar siempre, por regla general, con autorización del titular de forma previa e informada al tratamiento de datos, de la manera en la que lo dispone su artículo noveno.

Sin embargo, existen casos taxativos en los que no resultaría necesaria la autorización del titular y se encuentran contenidos en el artículo subsiguiente, cuando se trata de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
- Datos de naturaleza pública;
- Casos de urgencia médica o sanitaria;
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
- Datos relacionados con el Registro Civil de las Personas. (Ley 1581, 2012, art. 10).

De manera adicional, se impuso en los artículos 17 y 18 una serie de deberes a cargo tanto de los responsables como de los encargados del tratamiento respectivamente. En los deberes de los Responsables del Tratamiento de datos personales, se incluye garantizar el

ejercicio del derecho de hábeas data al titular, e informar a este sobre la finalidad de la recolección de datos, al igual que conservar la información de forma segura, garantizar la veracidad de los datos, tramitar consultas y reclamos formulados en los términos que disponga la ley. En los deberes de los encargados, se reiteran muchos de los ya mencionados en el acápite de los responsables, en tanto son concernientes a ambos sujetos, no obstante, se hace el llamado de adoptar políticas internas en cumplimiento de la ley, registrar reclamos en trámite, informar sobre violaciones de seguridad, y cumplir con instrucciones de la autoridad competente. Menciona el parágrafo del artículo 18 que, en caso de que una misma persona sea Responsable y Encargado del Tratamiento, deberá cumplir con los deberes de ambos roles.

Por otra parte, la regulación y manejo de información contenida en bases de datos financiera, crediticia, comercial, de servicios, ya se venía desarrollando desde un poco antes en la ley 1266 de 2008, que fue parcialmente reglamentada por el Decreto 1081 de 2015 y que se encargó de desarrollar el derecho contenido en el artículo 15 de la constitución, no solo como lo que prevé el texto constitucional, sino también como el derecho de toda persona a acceder, actualizar y corregir la información que se haya recopilado sobre ella en bases de datos, así como otros derechos, libertades y garantías constitucionales relativos a la recolección, manejo y circulación de datos.

El factor diferencial en las dos leyes mencionadas, consiste en que la ley 1581 de 2012 consagra disposiciones para el tratamiento de datos personales, mientras la ley del 2008 al ser su progenitora propone principios para la administración de datos de una manera general, que se reflejan en su sucesora. Los únicos principios que no se encuentran contenidos en la ley de 2012, son:

> d) Principio de temporalidad de la información. En ningún caso la información se podrá suministrar a terceros una vez cumpla la finalidad con la que fue recolectada. (Ley 1266, 2008, art.4).

> e) Principio de interpretación integral de derechos constitucionales. Cuando se haga la aplicación de esta ley, deberá hacerse haciendo observancia de todos los derechos relacionados, tales como hábeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. (Ley 1266, 2008, art.4).

Resulta también importante revisar el artículo séptimo del documento de ley del 2008, para efectos de la presente investigación, ya que es en este, dónde el legislador impone el deber a las entidades, empresas, etc, de tener reglamentado un procedimiento para el acceso a los datos y en qué términos podrá hacerse, entre otras disposiciones:

> **ARTÍCULO 7°.** (…) los operadores de los bancos de datos están obligados a:
>
> **(…**)
>
> **4**. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.
>
> **(**…)
>
> **11.** Cumplir las instrucciones y requerimientos que la autoridad de vigilancia imparta en relación con el cumplimiento de la presente ley. **(…)** (Ley 1266, 2008, art. 7).

Otro de los aportes relevantes de la ley tiene que ver con la enunciación taxativa en el artículo quinto, de los sujetos que pueden acceder a información contenida en bases de datos y bajo que presupuestos:

> **a)** A los titulares, personas que estén autorizadas por ellos y a sus causahabientes.
>
> **b)** A los usuarios de la información.
>
> **c)** A cualquier autoridad judicial, cuando medie orden judicial.

> **d)** A las entidades públicas del poder ejecutivo, cuando el conocimiento de la información corresponda al cumplimiento de alguna de sus funciones.
>
> **e)** A los órganos de control y demás dependencias de investigación disciplinaria, fiscal, o administrativa, cuando sea necesaria para una investigación en curso.
>
> **f)** A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad que la que tiene el operador que entrega los datos.
>
> **g)** A otras personas autorizadas por la ley. (Ley 1266, 2008, art.4).

Finalmente, en ambas leyes se hace un llamado a la Superintendencia de Industria y Comercio, entidad con la tarea de vigilar la protección de Datos e imponer las sanciones respectivas de encontrarse un incumplimiento de las disposiciones que ha previsto el legislador.

En el marco de las funciones que se le atañen a la SIC, en septiembre de 2016 expidió la Guía “PROTECCIÓN DE DATOS PERSONALES EN SISTEMAS DE VIDEOVIGILANCIA”, que resulta de vital importancia para tener en cuenta en el curso de esta investigación, para un acercamiento más directo a la solución que se busca dar al problema plateado.

En dicha guía la SIC explica como la grabación y monitoreo de personas a través de sistemas de videovigilancia implica la recolección de datos personales de que habla la ley 1581 de 2012 en su artículo tercero “Por la cual se dictan disposiciones generales para la protección de datos personales”, entendido como “(c)ualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables” (Ley 1581, 2012, art. 3). En este sentido, el tratamiento de datos (imágenes y videos) donde aparezcan sujetos determinables, deberá guardar respeto de los principios establecidos en dicha ley y demás disposiciones previamente mencionadas.

La SIC menciona que esta guía va dirigida en primer lugar, a personas, empresas, entidades u organizaciones que utilizan sistemas de videovigilancia para recolectar datos personales, ya sea como Responsables o Encargados del Tratamiento de estos datos. Esto incluye el uso de cámaras analógicas o digitales, cámaras IP, mini-cámaras, sistemas de circuito cerrado de televisión (CCTV) y cualquier otro medio que implique el tratamiento de imágenes de personas para fines de vigilancia, con el objetivo de orientarlos sobre sus obligaciones en materia de protección de datos personales. Esta guía también está dirigida a los Titulares de la información, personas cuyos datos son recopilados por estos sistemas de video vigilancia; su propósito es informarles sobre cómo ejercer sus derechos frente a quienes recolectan y manejan sus datos

Empresas como ESSA, que utilizan sistemas de videovigilancia como los CCTV con fines de seguridad, deberán acogerse a lo indicado en esta guía y demás disposiciones, dictadas por la SIC, siendo este último, ente garante de la protección del tratamiento de datos personales.

En esta guía se encuentra expreso que, en caso de que el titular de los datos (generalmente un empleado) desee acceder a la información que repose suya en las bases de datos de los SV podrán hacerlo y los responsables y encargados del tratamiento, deberán garantizarlo en líneas generales.

Entre las medidas tendientes que pudieran adoptarse para facilitar el acceso, indica la SIC que serían por ejemplo, reglamentar un protocolo para el acceso de imágenes y videos que permita verificar la titularidad de quien solicita el dato; exigir al titular fecha, lugar, hora, etc, para ser muy específicos a la hora de buscar y seleccionar el material y proteger al máximo la exposición de terceros; en caso de que en las imágenes concurran inevitablemente terceros, se deben utilizar todas las herramientas necesarias para procurar su anonimización a la hora de entregar el material, esto en el caso de que no se cuente con la autorización de estos terceros (SIC, Protección de datos personales en sistemas de videovigilancia, 2016).

Son estos unos lineamentos muy valiosos a la hora del acceso del titular datos tales como imágenes y videos, pero se quedan cortos al momento de tratar casos específicos, un claro ejemplo de ellos, el procedimiento disciplinario laboral, ya que aquí no solamente se requiere del “acceso”, si no también se requiere que los datos sean suministrados para que posteriormente el trabajador pueda usarlos a su favor o controvertirlos en el curso de su defensa técnica.

Aun así, es clara la SIC al reiterar que la tarea de diseñar y reglamentar protocolos internos de cada empresa o entidad corresponde en ultimas a las mismas. También termina dando unas recomendaciones como ayuda a la hora de elaborar estos, como el hecho de prestar atención a las disposiciones contenidas en el Régimen General de Protección de Datos Personales.

2.2 Estado del arte

2.2.1. Intimidad y protección de datos como derechos vertebradores en el uso de dispositivos de videovigilancia en el lugar de trabajo (González, 2020).

Este trabajo será de ayuda para analizar la discusión que ha girado en torno al dilema planteado inicialmente con una perspectiva internacional, en tanto, trata temas sobre el uso de sistemas de videovigilancia en los espacios de trabajo y la legitimidad que tienen los datos recolectados por estos, al momento de ser usados como prueba procesal en el régimen español.

2.2.2. El debido proceso en la ley de habeas data (Gil Cifuentes, 2017).

Este articulo científico elaborado por un abogado especialista en derecho procesal de la Universidad de Antioquia, hace un recuento del derecho al debido proceso, partiendo de la estructura de Colombia como Estado Social de derecho, explicando la relación de tensión que tiene con la ley de habeas data, haciendo una línea jurisprudencial en materia del tema de estudio.

2.2.3. Debido proceso y procedimiento disciplinario laboral (Tejada, 2016).

Este artículo publicado en la revista Opinión Jurídica de la Universidad de Medellín, será de ayuda para entender cómo debe realizarse un proceso disciplinario empresarial, que aplique los principios del debido proceso, permitiendo la no vulneración de los derechos de los trabajadores puesto que, incluso los trámites administrativos internos no se encuentran exentos de aplicar las garantías constitucionales.

2.2.4. El alcance de la subordinación frente al derecho de la intimidad y al habeas data en un contrato laboral en Colombia (Restrepo, 2020).

Una tesis de la Pontificia Universidad Javeriana que estudia los límites de la subordinación laboral y como esta puede ser violatoria a los derechos a la intimidad y el habeas data, cuando el empleador se extralimita en sus facultades, en el marco del desarrollo de un contrato de trabajo.

2.2.5. La protección de datos personales frente a los sistemas de vídeo vigilancia en Colombia (Beltrán, 2016).

Trabajo de grado de la Universidad Gran Colombia, que nuevamente plantea la problemática del derecho a la protección de datos frente al uso de sistemas de videovigilancia,

enfocado en el régimen colombiano y que servirá para entender si existe o no violación de derechos cuando cámaras de vídeo vigilancia recaban datos personales sin autorización del titular.

2.3 Marco conceptual

Para entender el caso en concreto en materia jurídica, es importante tener claridad de los siguientes conceptos, dado que algunos de estos no son propiamente del derecho, pero resultan relevantes para la investigación jurídica.

Debido Proceso: El derecho al debido proceso, además de estar garantizado en el artículo 29 de la Constitución Política, se encuentra protegido en diversas normas internacionales y tratados que el país ha suscrito. El Comité de Derechos Humanos de las Naciones Unidas enfatiza la necesidad de establecer normas que aseguren la igualdad ante los tribunales y cortes de justicia, así como el derecho de toda persona a ser escuchada con las debidas garantías por un tribunal competente, independiente e imparcial, creado conforme a la ley. La Corte Constitucional en la sentencia T-516 de 1992, destacó que el derecho al debido proceso abarca tanto los procesos judiciales como administrativos y el respeto a las formalidades específicas de cada juicio, en función de los principios que los orientan, los intereses en disputa y las cualidades de los jueces y funcionarios encargados de tomar las decisiones.

Derecho a la contradicción y defensa: Este derecho, tal como se definió en la Sentencia T-051 de 2016, garantiza a toda persona la posibilidad de ser escuchada, de presentar sus argumentos, de impugnar o contradecir las pruebas en su contra, de solicitar la práctica y evaluación de pruebas que le favorezcan, así como de ejercer los recursos que la ley le otorga dependiendo de la situación. Desde un enfoque doctrinario, este derecho asegura

la participación de las partes (diferentes al juez) en los procesos judiciales, permitiéndoles exponer sus argumentos y presentar pruebas. Además, se desglosa en dos derechos específicos: el de contradicción y el de defensa técnica.

Habeas data: Este derecho se basa en que toda persona tiene la potestad de conocer, actualizar y corregir la información que repose sobre ella en bases de datos, tanto públicos como privados. La Corte Constitucional lo ha definido como la facultad de los titulares de los datos para exigir a las entidades que los administran, el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de dichos datos, así como limitar su divulgación, publicación o cesión, de acuerdo con la regulación en materia de datos personales. Este derecho es independiente, aunque relacionado con otros derechos como intimidad e información. Es fundamental que ninguna entidad sin importar su carácter no incumpla la Ley 1581 de 2012, que regula la protección de este derecho, ya que la mayoría de las organizaciones manejan bases de datos de clientes, proveedores o empleados.

Titular de la información: Se refiere a la persona natural o jurídica sobre la cual se almacena información en una base de datos. Por ejemplo, un usuario que haya firmado un contrato de prestación de servicios de comunicaciones. Los titulares tienen el derecho de acceder a las imágenes tratadas a través de sistemas de videovigilancia (SV). (SIC, sitio web).

Datos de carácter sensible: Estos son datos personales, como las imágenes de los titulares, se consideran biométricos y sensibles cuando son procesados mediante técnicas específicas que permiten la identificación o autenticación única de una persona. En caso contrario, son simplemente datos personales de carácter privado (SIC, Concepto No. 18-171259 del 27 de julio de 2018).

Tratamiento de datos: Según la Ley 1581 de 2012, es cualquier operación realizada sobre datos personales, como la recolección, almacenamiento, uso, circulación o supresión. Las acciones que involucran imágenes de personas identificadas o identificables, como su captura, grabación, transmisión, almacenamiento, conservación o reproducción, corresponden a tratamiento de datos personales y están obligadas a respectar a la normativa general de protección de datos ya mencionada.

Responsable del tratamiento: Es la persona natural o jurídica que decide los fines y formas de manejar los datos personales, asegurando en todo momento el ejercicio completo del derecho de habeas data, protegiendo la seguridad de la información para prevenir su alteración, pérdida, consulta, uso o acceso no autorizado, y realizando las actualizaciones, rectificaciones o supresiones de los datos cuando sea necesario o los titulares lo exijan. (Ámbito Jurídico, sitio web).

Información pública: De acuerdo con la Sentencia T-427 de 2013 de la Corte Constitucional de Colombia, se refiere a aquella información que cualquier persona puede

solicitar directamente, sin necesidad de cumplir requisitos específicos. Esta categoría incluye, por ejemplo, actos normativos de carácter general, decisiones judiciales en firme y datos relacionados con el estado civil de los individuos, etc. (Sentencia T-427 de 2013).

Información semiprivada: Tiene un nivel mínimo de restricción y solo puede ser obtenida o divulgada por orden de una autoridad administrativa en el marco de sus funciones, por ejemplo, datos relacionados con entidades de seguridad social o comportamiento financiero (Sentencia T-427 de 2013).

Información privada: Incluye datos personales o impersonales que, por estar en un ámbito privado, solo pueden obtenerse o divulgarse por orden de una autoridad judicial, como libros de comerciantes, documentos privados, historias clínicas o información derivada de la inspección de un domicilio (Sentencia T-427 de 2013).

Información reservada: Comprende datos personales vinculados directamente a derechos fundamentales como la dignidad, libertad o intimidad, por lo que no pueden ser obtenidos ni divulgados ni siquiera por una autoridad judicial, tal como ocurre con información genética u orientación sexual. (Sentencia T-427 de 2013).

Sistemas de videovigilancia (SV): Estos sistemas se consideran intrusivos de la privacidad, por lo que deben ser implementados solo cuando sea absolutamente necesario y no existan alternativas menos invasivas que puedan cumplan el mismo objetivo. Su uso está vinculado al principio de finalidad que requiere que el tratamiento de datos personales sea conforme a la Constitución y la ley, y persiga un propósito específico, explícito e informado. Cualquier cambio en las finalidades establecidas requiere la autorización de los titulares de los datos para su continuidad. (Superintendencia de Industria y Comercio [SIC], 2016).

CCTV: Un sistema de circuito cerrado de televisión (CCTV) es un conjunto de dispositivos interconectados que generan un circuito cerrado de imágenes accesible solo para un grupo específico de personas, utilizados para seguridad, vigilancia o mejora de servicios. Su configuración incluye cámaras, transmisores o cables para enviar la señal de video, y monitores para visualizar las imágenes. (SECURICORP, sitio web).

Proceso disciplinario laboral: Es el procedimiento que una empresa debe seguir para investigar y aclarar presuntas faltas cometidas por sus empleados. Durante este proceso, el trabajador tiene la oportunidad de ser escuchado, de refutar las pruebas presentadas por el empleador y de aportar sus propias pruebas, antes de que el empleador decida si impone una sanción disciplinaria. Este proceso está regulado en el artículo 115 del Código Sustantivo del Trabajo, que establece que antes de aplicar una sanción, se debe dar la oportunidad de ser escuchado tanto al trabajador que está siendo inculpado como a dos representantes del sindicato al que este afiliado este. (Código Sustantivo del Trabajo, 1950, art 115).

3. Desarrollo

3.1 Elementos doctrinales entorno al proceso laboral disciplinario.

Este informe al ser la etapa inicial de la investigación entenderá cómo funciona el procedimiento disciplinario que se lleva al interior de una empresa, así como su fundamento legal y jurídico. En este punto es importante precisar que para el caso de ESSA, existen dos Convenciones Colectivas de Trabajo (CCT) actualmente vigentes (SIPROESSA y SINTRAELECOL) las cuales rigen el proceso disciplinario dependiendo de la afiliación al sindicato que tenga el trabajador, de no pertenecer a ninguno, simplemente se aplican las disposiciones del Reglamento Interno de Trabajo (RIT).

El informe también comprenderá las características y diferencias que comparte con un proceso disciplinario con uno judicial. Todo lo anterior con el objetivo de brindar un contexto al lector sobre las temáticas que se desarrollarán en los siguientes informes.

A continuación, se explicarán los procedimientos internos disciplinarios existentes en ESSA mediante el uso de diagramas de flujo. Posteriormente se hará el análisis pertinente con relación al proceso laboral disciplinario en Colombia.

Figura 4.

Proceso Disciplinario Reglamento Interno de Trabajo ESSA

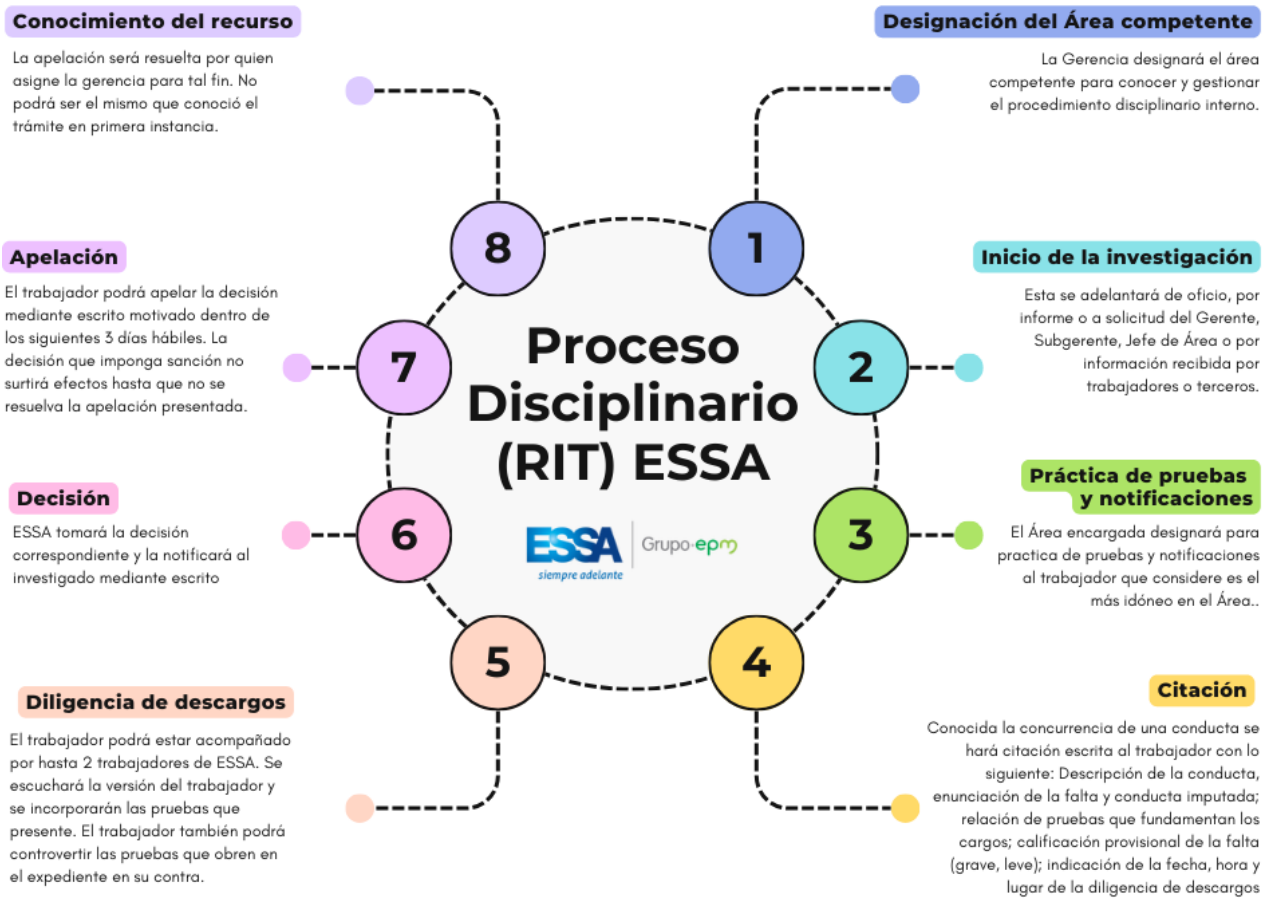


Figura 5.

CCT ESSA SINTRAELECOL

Figura 6.

CCT ESSA SIPROESSA

Para hablar del proceso laboral disciplinario se debe partir entendiendo los elementos esenciales del contrato de trabajo. El único que se abordará por ser de utilidad para este análisis, es la Subordinación.

3.1.1. Subordinación

Este elemento distintivo y determinante del contrato de trabajo, ha sido entendido por la Corte Constitucional en su sentencia C-386 de 2000 como "un poder jurídico permanente de que es titular el empleador para dirigir la actividad laboral del trabajador, a través de la expedición de órdenes e instrucciones y la imposición de reglamentos” esto con el objetivo se estar al tanto de como “debe realizar las funciones y cumplir con las obligaciones que le son propias, con miras al cumplimiento de los objetivos de la empresa, los cuales son generalmente económicos" (Corte Constitucional de Colombia, Sentencia C-386, 2000).

Por otro lado, esta misma Corte expresó en la Sentencia C-934 de 2004 que dentro del elemento de la subordinación se encuentra la facultad de poder dirigir las actividades laborales llevadas al interior de la organización, así como la potestad de la función disciplinaria de ser necesario para aplicar las medidas correctivas tendientes a poder mantener “el orden y la disciplina en su empresa”. Sin embargo, aclara la corte que la facultad disciplinaria solo podrá predicarse en lo relativo a las actividades estrictamente laborales y sus esferas propias derivadas de la relación entre empleador y trabajador, de igual manera este poder sancionatorio no es absoluto y mucho menos podrá usarse de manera arbitraria frente a los trabajadores (Corte Constitucional de Colombia, Sentencia C-934, 2004).

Teniendo de presente los conceptos mencionados, aceptados por doctrina y jurisprudencia reiterada se entiende entonces que, se le confiere al empleador facultades coercitivas, de instrucción y de mando que permiten reglamentar únicamente lo concerniente a la actividad laboral que realiza el trabajador; de acá mismo se desprende la facultad disciplinaria que ostenta el empleador sobre el trabajador dado que, en el curso de la actividad laboral a desempeñar muchas veces es necesario verificar y vigilar la correcta función de

esta, así como advertir un error si lo hubiere, amonestar e incluso sancionar si hay ocasión a una falta al deber encomendado al empleado. Se entiende también como un medio para tomar acciones correctivas sobre los trabajadores que incumplen el contrato de trabajo o el reglamento interno de una empresa.

No obstante, la facultad disciplinaria no puede en ningún caso considerarse absoluta y deberá estar sujetada a límites internos o funcionales (precisado en alguna clase de reglamento), y a límites externos o jurídicos, es decir, a los principios que rigen el derecho fundamental al debido proceso, consagrados constitucionalmente y que se explicarán más adelante.

3.1.2. El debido proceso, visión general

La jurisprudencia constitucional ha delimitado el derecho al debido proceso como el conjunto de garantías establecidas en el ordenamiento jurídico que están diseñadas para proteger a las personas inmersas en actuaciones judiciales o administrativas. Su propósito es asegurar que se respeten los derechos de su persona (sea jurídica o natural) durante el proceso y lograr una correcta administración de justicia. Algunas de las garantías del debido proceso incluyen:

(i) El derecho a la jurisdicción, que se refiere al acceso libre e igualitario a la justicia, que abarca no solo los jueces sino también autoridades administrativas; así como a obtener por parte de estas decisiones motivadas, con posibilidad de poderlas impugnar e incluso garantizar su cumplimiento

(ii) el derecho al juez natural, identificado como la persona capacitada y con la aptitud legal necesaria para resolver un conflicto dependiendo de la naturaleza de este y la división del trabajo establecida por la Constitución y la ley;

(iii) El derecho a la defensa, como la facultad de ser escuchado en aras de obtener una decisión que le favorezca. Comprende también, el derecho tener el tiempo para expresar las ideas y disponer de los medios adecuados para la preparación de una

adecuada defensa; los derechos de ser asesorado y representado por un abogado cuando sea necesario, la igualdad ante la ley procesal, la buena fe y la lealtad de todas las personas que hacen parte del proceso;

(iv) el derecho a un proceso público, que se desarrolle en un tiempo razonable, lo que conlleva que el proceso no se vea afectado por una dilatación injustificable;

(v) el derecho a la independencia del juez, es decir, que quienes tienen la misión de administrar justicia se encuentren separados del poder ejecutivo y legislativo.

(vi) el derecho a la independencia e imparcialidad del juez o funcionario, el juez deberá impartir justicia de manera imparcial y sin ser influenciado por factores o personas externas. (Corte Constitucional de Colombia, Sentencia C-341, 2014).

3.1.3. El debido proceso laboral disciplinario

El ejercicio de los poderes que tienen el empleador sobre sus trabajadores ha sido entendido por la Corte Constitucional en la Sentencia C-386 de 2000 de la siguiente manera: "Los poderes del empleador para exigir la subordinación del trabajador, tienen como límite obligado el respeto por la dignidad del trabajador y por sus derechos fundamentales". (Corte Constitucional de Colombia, Sentencia C-386, 2000).

Esta interpretación hace casi una remisión directa a la Constitución en el artículo 29, que se ha explicado previamente y del cual se destaca el inciso que menciona: "El debido proceso se aplicará a toda clase de actuaciones judiciales y administrativas", lo que deja claro que el proceso laboral disciplinario también debe ser observante de este principio.

De igual manera, el artículo 29 expresa que el debido proceso está conformado por unos principios generales del derecho, tales como el “Principio de Legalidad, el Principio de Congruencia, el Principio de Proporcionalidad, el Principio Non Bis In Ídem, la Presunción de Inocencia y el Derecho a la Defensa” (Const., 1991), los cuales resultan relevantes para

este análisis debido a su trascendencia al momento de realizar el procedimiento disciplinario. A continuación, se explicará uno a uno.

3.1.4. Principio de Legalidad

Implica que “Nadie podrá ser juzgado sino conforme a leyes preexistentes al acto que se le imputa”. (Const., 1991) La Corte se ha referido a este principio en materia penal como disciplinaria en la Sentencia C-124 de 2003 indicando que comporta la “salvaguarda de la seguridad jurídica de los ciudadanos” y que involucra el conocimiento de todo lo que está prohibido, es decir, qué comporta un delito o falta, así como las penas y sanciones que se aplicaran, sea en un proceso penal o disciplinario. Este principio también es un garante de la libertad individual. De igual manera protege a las personas de las actuaciones arbitrarias por parte de autoridades judiciales o administrativas y propende la igualdad de todas las personas ante el poder punitivo y sancionatorio del Estado. La Corte manifestó que el debido proceso en cuanto a este principio constitucional supone “la legalidad de la conducta sancionada y de la pena a imponer”. (Corte Constitucional de Colombia, Sentencia C-124, 2003).

Desglosándolo en el ámbito disciplinario, este principio implica que los trabajadores solo podrán ser investigados y sancionados con ocasión a faltas que estén previamente establecidas en los reglamentos internos de cada empresa o que violen disposiciones legales o contractuales (el contrato es ley para las partes). Así mismo, la investigación disciplinaria que se lleve a cabo debe estar orientada a demostrar que efectivamente se cometió la falta.

3.1.5. Principio de Congruencia

Este principio tiene que ver con la correlación entre la acusación y el fallo, es decir, la existencia de un nexo causal. Está constituido como una de las garantías más importantes de un debido proceso; en términos sencillos, la decisión que se tome no podrá recaer sobre hechos diferentes a los que se presentaron en la acusación.

Por su parte, la Corte Suprema de Justicia estableció en la Sentencia 24668 del 06 de abril de 2006 que un juez o autoridad sancionatoria, podría transgredir este principio de dos maneras, por acción u omisión. En el primer caso “Cuando se condena por hechos distintos a los contemplados en la formulación de imputación o de acusación” o también “Cuando se condena por un delito que nunca se hizo mención fáctica ni jurídicamente en el acto de formulación de imputación o de la acusación”. En el segundo caso, relativo a la omisión “Cuando en el fallo se suprime una circunstancia, genérica o específica, de menor punibilidad que se hubiese reconocido en las audiencias de formulación de la imputación o de la acusación”. (Corte Suprema de Justicia de Colombia, Sentencia 24668, 2006).

Ahora, haciendo un desplazamiento de estos conceptos originalmente del derecho penal al laboral disciplinario, este principio se vulnera en las siguientes situaciones:

1. Se condena por hechos distintos a los reportados inicialmente.
2. Cuando se sanciona por una falta que no se configura con los hechos reportados.
3. Cuando se omiten las circunstancias que implicarían una sanción menor para el infractor (Tejada Correa, 2016).

En este sentido, es labor de las empresas estructurar la manera en que deben iniciarse las investigaciones disciplinarias, bien sea mediante una comunicación directa del jefe del área encargada o de oficio por información que provenga de cualquier persona de la organización o entidad.

3.1.6. Principio de proporcionalidad

Este principio guarda conexión con el de congruencia, sin embargo, acá la relación entre los hechos y la sanción a imponer debe leerse de manera aún más estricta, pues la

gravedad de la sanción debe ser proporcionalidad a la gravedad de la falta, siendo necesario no solo analizar los hechos ocurridos, sino también la trascendencia de estos y las condiciones del trabajador, convirtiéndose un principio que delimita la potestad disciplinaria del empleador.

Según la Corte Constitucional en la Sentencia C-822 de 2005, este principio se basa en la relación circunstancial entre hecho y consecuencia jurídica. Se encarga este de analizar la gravedad entre la conducta delictiva y la pena o sanción a imponer, así como causales que puedan configurar un agravamiento, atenuación o graduación de la pena, o inclusive la magnitud de la afectación al bien tutelado, el daño antijurídico provocado y la sanción pecuniaria correspondiente a pagar. (Corte Constitucional de Colombia, Sentencia C-822, 2005).

En ultimas, este principio se asegura de que la autoridad disciplinaria, siempre actúe dentro de lo que corresponde al Estado de Derecho, sin extralimitarse en sus funciones.

Como consecuencia de la aplicación de este principio, se debe revisar con cuidado los factores que pueden incrementar o disminuir la gravedad de la falta concurrida. Por otro lado, que las sanciones que se hayan impuesto de forma objetiva por situaciones particulares implican que en el futuro en casos similares se apliquen sanciones equiparables, solo podrían variar en el caso de que se presenten circunstancias atenuantes o agravantes.

3.1.7. Principio Non Bis In Ídem

Este principio se manifiesta como el derecho a no ser juzgado dos veces por el mismo hecho. La jurisprudencia de la Corte Constitucional en la Sentencia T-537 de 2002 sostuvo que gracias a este principio las personas pueden tener la certeza de que las decisiones y fallos emitidos con ocasión a los procesos cursados en su contra, una vez cursadas las instancias procesales a que hubiera lugar dependiendo del caso, son definitivos y no se permitirá que

por los mismos hechos sean juzgados y objeto de futuros debates. “El principio *non bis in ídem* es una manifestación de la seguridad jurídica y una afirmación de la justicia material" (Corte Constitucional de Colombia, Sentencia T-537, 2002).

Con esta definición, la Corte establece que el principio *non bis in ídem* protege tanto la seguridad jurídica como la justicia material, evitando la duplicidad de juicios sobre los mismos hechos. Este principio tiene una relevancia fundamental en el derecho penal y disciplinario, garantizando que una persona no sea sometida a múltiples procesos por la comisión de una misma conducta.

3.1.8. Presunción de Inocencia

Este principio se resume sencillamente en que toda persona se presumirá inocente mientras no se la haya declarado judicialmente culpable. Este derecho está reconocido constitucionalmente en el artículo 29 inciso cuarto de la Carta Política, que establece: “Toda persona se presume inocente mientras no se la haya declarado judicialmente culpable” (Const., 1991).

Siguiendo esta interpretación constitucional, la Corte Suprema de Justicia, en la Sentencia No. 22179 del 9 de marzo de 2006, ampara la presunción de inocencia indicado que no puede haber ninguna clase de juicio premeditado de parte del juez y que de cualquier manera, el investigado, no tiene el deber de presentar ninguna prueba que permita acreditar su inocencia, sino que el proceso debe iniciar presumiéndola, ya que son en ultimas las autoridades judiciales quienes deben desvirtuar probatoriamente esta. (Corte Suprema de Justicia de Colombia, Sentencia No. 22179, 2006, M.P. Alfredo Gómez Quintero).

Este principio no escapa de ninguno de los órdenes sancionatorios, incluido el disciplinario, por lo que deberá ser respetado en los procedimientos disciplinarios que se tengan dentro de las empresas.

De igual manera, implica que toda duda que surja con relación a la comisión de una conducta sancionable deberá resolverse a favor del trabajador, puesto que es en ultimas el órgano sancionador quien tiene la tarea de reunir todas las pruebas necesarias para demostrar que efectivamente se cometió la falta, previo al fallo disciplinario, tales como testigos, documentos, grabaciones, etc.

3.1.9. Derecho de Defensa

De manera simple, este corresponde a toda exposición de argumentos facticos y jurídicos tendientes a desvirtuar la acusación. En el ámbito disciplinario tiene que ver, con brindar la oportunidad de manifestarse frente a los hechos y pruebas que se hayan presentado en su contra en el marco de una investigación disciplinaria, así como su versión de los hechos. Cobra tanta importancia, que el desconocimiento de este derecho repercute en que se deje sin efectos la sanción que se hubiera impuesto.

Según Suárez (1999), el derecho a la defensa implica además, el derecho del imputado a ser informado de manera específica y clara sobre los hechos que se le imputan. También abarca la aplicación del principio de contradicción en todas las fases procesales y el derecho a presentar sus alegaciones, es decir, a exponer los elementos de hecho y de derecho que puedan influir en el resultado final, así como a probarlos. Por último, la motivación de la sentencia es también una manifestación positiva del derecho a la defensa” (Suárez, 1999, p. 356).

En consonancia con los principios analizados que conforman el debido proceso, la Corte ha expresado mediante la Sentencia T-301 de 1996 una serie de mínimos que en términos generales, se deberían respetar en todas las etapas del procedimiento disciplinario, sin importar el carácter de este:

(1) la comunicación formal de la apertura del proceso disciplinario a la persona a quien se imputan las conductas pasibles de sanción.

(2) la formulación de los cargos imputados, que puede ser verbal o escrita, siempre y cuando en ella consten de manera clara y precisa las conductas, las faltas disciplinarias a que esas conductas dan lugar (con la indicación de las normas reglamentarias que consagran las faltas) y la calificación provisional de las conductas como faltas disciplinarias.

(3) el traslado al imputado de todas y cada una de las pruebas que fundamentan los cargos formulados.

(4) la indicación de un término durante el cual el acusado pueda formular sus descargos (de manera oral o escrita), controvertir las pruebas en su contra y allegar las que considere necesarias para sustentar sus descargos.

(5) el pronunciamiento definitivo de las autoridades competentes mediante un acto motivado y congruente.

(6) la imposición de una sanción proporcional a los hechos que la motivaron; y (7) la posibilidad de que el encartado pueda controvertir, mediante los recursos pertinentes, todas y cada una de las decisiones de las autoridades competentes. (Corte Constitucional de Colombia, Sentencia T-301, 1996).

3.1.10. La facultad sancionatoria del empleador desde lo legislativo

Luego de haber hecho un análisis jurisprudencial de los principios que son aplicables y conforman lo que se entiende por debido proceso disciplinario laboral, además de haber explicado el fundamento del poder sancionatorio desde la perspectiva de la doctrina jurídica, es importante conocer cuáles son las normas que se encargan de amparar y regularlo.

El artículo 111 del Código Sustantivo del Trabajo establece que "Las sanciones disciplinarias no pueden consistir en penas corporales, ni en medidas lesivas de la dignidad del trabajador" (Código Sustantivo del Trabajo de Colombia, 1950).

Asimismo, el artículo 114 del mismo código menciona que "El empleador no puede imponer a sus trabajadores sanciones no previstas en el reglamento, en pacto, en convención colectiva, en fallo arbitral o en contrato individual" (Código Sustantivo del Trabajo de Colombia, 1950).

Estos artículos, junto con los comprendidos entre el 111 y el 115 del mismo código, hacen una alusión directa a las sanciones y multas que puede imponer un empleador cuando un trabajador ha cometido una falta. Al revisar estos artículos, destaca el artículo 115, que se analizará a continuación:

> "Antes de aplicarse una sanción disciplinaria, el empleador debe dar oportunidad de ser oídos tanto al trabajador inculpado como a dos representantes del sindicato al que este pertenezca. No producirá efecto alguno la sanción disciplinaria que se imponga pretermitiendo este trámite" (Código Sustantivo del Trabajo de Colombia, 1950).

Esta disposición está incluida en el Título IV, Capítulo I del CST, que regula la existencia del Reglamento Interno de Trabajo como el conjunto de normativas que establecen las condiciones bajo las cuales el empleador y sus trabajadores deben operar durante la prestación del servicio. Esta medida es obligatoria para aquellas empresas que tengan más de cinco trabajadores de forma permanente en el sector comercial, más de diez en el sector industrial, o más de veinte en el sector agrícola, ganadero o forestal.

En la Sentencia C-593 de 2014, la Corte Constitucional hace un análisis específico de esta disposición y encuentra que pueden darse dos interpretaciones: una contraria al derecho al debido proceso consagrado en nuestra Constitución, y otra acorde con las disposiciones del ordenamiento superior (Corte Constitucional de Colombia, Sentencia C-593, 2014).

Menciona que, al hacer una primera lectura, se podría interpretar que el artículo 115 simplemente requiere que se dé la oportunidad al trabajador de ser escuchado antes de imponer una sanción se encuentre el Reglamento de Trabajo, no obstante, esta interpretación de la norma resultaría contraria al derecho al debido proceso y a lo que se ha consagrado por doctrina constitucional referente a la necesidad de garantizar las prerrogativas inherentes al artículo 29 de la Constitución política en el campo de las relaciones laborales.

Por otro lado, la lectura correcta que debería hacerse de conformidad con el texto constitucional consiste en entender que, cuando el legislador dispone que deba escucharse al trabajador previamente a imponer una sanción, lo hace con el objetivo de que se respeten las garantías del debido proceso:

> “Recuerda la Sala que el referido derecho constitucional se aplica no sólo a las actuaciones judiciales y administrativas del Estado, sino que en todos los campos donde se haga uso de la facultad disciplinaria, entiéndase ésta como la prerrogativa de un sujeto para imponer sanciones o castigos para mantener el orden al interior de las organizaciones privadas. Ello, además, resulta de trascendental importancia cuando se trata de relaciones laborales en donde existe un alto grado de subordinación y el trabajador se constituye como la parte débil de dicha relación jurídica.” (Corte Constitucional de Colombia, Sentencia C-593, 2014).

En este sentido, se resalta nuevamente la necesidad de que el empleador siempre fije en su reglamento internos unos mínimos que permitan parametrizar y limiten claramente el alcance de su facultad sancionatoria; que se establezca un procedimiento que permita a los trabajadores acceder fácilmente y conocer tanto conductas que pueden repercutir en una falta, como la sanción en sí, aplicable a estas. A su vez, que se disponga de garantías que impidan la vulneración de derecho al debido proceso y la defensa de los trabajadores que hacen parte de la organización.

Predica también la mencionada sentencia que, cualquier sanción que se imponga al trabajador deberá estar contenida, primeramente, en el reglamento interno de trabajo y segundo, que la imposición de la sanción se entienda como el resultado de un debido proceso disciplinario en el que se haya oído en un momento anterior al trabajador, así como que se le haya brindado la posibilidad de presentar pruebas y controvertir las que hubiera en su contra. La decisión que se tome, deberá ser en derecho, debidamente motivada e indicar explícitamente la conducta imputada que dio ocasión a la falta en la que incurrió el trabajador. Ahora, dependiendo del caso particular y si es procedente, disponer de la posibilidad de que, si el trabajador así lo quisiera, la decisión pueda ser apelada y revisada por un superior jerárquico. (Corte Constitucional de Colombia, Sentencia C-593, 2014).

Además, el empleador debe ejercer su facultad de imponer sanciones de manera razonable y proporcional a la falta cometida, asegurándose de que los hechos imputados estén plenamente probados.

Los magistrados de la alta Corte en la sentencia de referencia C-593 de 2014, han manifestado que el artículo 115 del CST se debe interpretar como el deber del empleador de contar con un reglamento interno de trabajo en donde estén estipuladas de manera taxativa lo que se considera como falta, de forma anterior a la imposición de una eventual sanción, ello con el objeto de garantizar los principios que reglamentan el debido proceso. (Corte Constitucional de Colombia, Sentencia C-593, 2014).

3.1.11. Conclusión del primer informe

Tras la revisión jurídica y legislativa, se encuentra que uno de los elementos fundamentales del contrato de trabajo es el de subordinación, ya que dota al empleador de la facultad coercitiva y correctiva sancionatoria, que legislativamente se encuentra amparado en el Código Sustantivo del Trabajo. Por otra parte, al momento de iniciar una investigación

disciplinaria de carácter laboral se deberán de tener en cuenta todos los elementos que giran en torno al debido proceso por regla general, ya que se trata de principios orientadores que se han desarrollado mediante jurisprudencia en múltiples ocasiones, lo que los hace doctrina consagrada.

3.2. Análisis de toda la regulación colombiana en materia de tratamiento y suministro de datos

Teniendo claros los elementos doctrinantes que rigen el proceso laboral disciplinario revisados en el primer informe, y prosiguiendo con los objetivos del trabajo de investigación, en este segundo informe se analizará el panorama actual colombiano en materia de suministro y tratamiento de datos, en especial los de carácter sensible, con el fin de conocer toda la normatividad que rige actualmente en el país.

De acuerdo con la jurisprudencia de la Corte Constitucional, la propia Constitución y la Ley 1581 de 2012, junto con sus decretos reglamentarios, la autorización o autodeterminación informática es considerada el fundamento esencial del habeas data. Esta autorización debe ser libre, previa y expresa, salvo mandato legal o judicial que establezca lo contrario. La inexistencia de esta autorización implica una violación directa del Derecho Fundamental a la Protección de Datos Personales o intimidad.

A continuación, se desglosará de a poco el Derecho Fundamental a la Protección de datos personales o intimidad y su relación con el tratamiento de imágenes en sistemas de videovigilancia.

Primeramente, este derecho puede definirse como la facultad que tiene toda persona de decidir y conocer sobre sus datos personales, incluyendo la identificación del responsable

y encargado del tratamiento de los datos, el tipo de tratamiento que realiza, quiénes tienen acceso a esa información, las medidas de seguridad que se aplican para su protección, así como las condiciones presentes y futuras del procesamiento de dichos datos, y, en general, los principios que rigen su regulación.

En este punto, es importante precisar qué se considera o entiende por dato personal. La Ley Estatutaria 1581 de 2012 lo define como “cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables” (Ley 1581, 2012, art. 3).

De igual manera, la jurisprudencia de la Corte Constitucional, en la Sentencia C-748 de 2011, indicó lo que a su criterio caracteriza a un dato personal:

> “i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación” (Corte Constitucional de Colombia, Sentencia C-748, 2011)

Teniendo claro este concepto, recordemos nuevamente la definición de “tratamiento” y “base de datos” conforme a la Ley 1581 de 2012. El tratamiento se define como “cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión”. La base de datos se refiere al “conjunto organizado de datos personales que sea objeto de tratamiento” (Ley 1581 de 2012, art. 3).

Acorde a la sentencia C-748 de 2011, las bases de datos comprenden “todo espacio donde se haga alguna forma de tratamiento del dato, desde su simple recolección, lo que

permite extender la protección del habeas data a todo tipo de hipótesis” (Corte Constitucional de Colombia, Sentencia C-748, 2011).

Entonces, poniendo las definiciones en retrospectiva con el caso que atiende a este trabajo de investigación, los Sistemas de Videovigilancia al captar imágenes de personas, vienen a hacer lo que se comprende como “tratamiento”, en tanto pueden identificar a esa persona y solo a ella, es decir captan o almacenan un “dato personal” en una base de datos; esto significa que el Derecho a la Protección de Datos Personales está directamente relacionado con los sistemas de videovigilancia, ya que estos cumplen con los dos supuestos principales: los datos personales y el tratamiento.

Continuando con el análisis de la Ley 1581 de 2012, uno de los aspectos más destacados es el contenido del primer inciso del artículo sexto: “El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización” (Ley 1581, 2012, art. 6). Es claro entonces, que al momento de realizar el tratamiento de datos personales es fundamental contar con la autorización del titular, ello en consonancia con la disposición del texto constitucional en el artículo 15, el cual establece el derecho de las personas a su intimidad personal y familiar, y a su buen nombre, así como la obligación de respetar las garantías constitucionales durante la recolección, tratamiento y circulación de los datos (Constitución Política de Colombia, 1991, art. 15).

Las únicas excepciones que existen con respecto a la autorización de los titulares son las contenidas en la Sentencia C-431 de 2003 y en el artículo décimo de la Ley Estatutaria 1581 de 2012, que son las siguientes:

> “(i) Actividades de incursión y seguimiento ejercida por las autoridades judiciales para impedir la ejecución o consumación de conductas punibles.

(ii) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;

(iii) Datos de naturaleza pública;

(iv) Casos de urgencia médica o sanitaria;

(v) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;

(vi) Datos relacionados con el Registro Civil de las Personas” (Corte Constitucional de Colombia, Sentencia C-431, 2003; Ley 1581, 2012, art. 10).

Análisis de la sentencia C 748 de 2011

Continuando con la discusión pertinente al tema objeto del trabajo, resulta necesario estudiar la Sentencia C-748 de 2011, sentencia de revisión que comprende claramente el alcance material de la ley estatutaria, puesto que refiere que independientemente de la finalidad que tenga una base de datos, mientras incluya información y datos personales, debe tener en cuenta la aplicación de los principios legales que previó el legislador para el tratamiento y protección de datos. Indica la Corte entonces lo relevante que es la ley 1581 de 2012 en esta tarea, en tanto no se puede pretender dejar una base de datos sin una legislación que le sea aplicable en materia de administración de datos, y si eventualmente llegase a ser el caso, deberá fundamentarse en un grueso de argumentación en el que se demuestre en su lugar la necesidad de aplicación de un test de razonabilidad, que tendrá el objetivo de demostrar por qué no le son aplicables los principios básicos desarrollados a partir de este derecho fundamental y sus derechos conexos. (Corte Constitucional de Colombia, Sentencia C-748, 2011).

La Corte también indica que dicha ley se limita a regular los aspectos del derecho al hábeas data y relacionados, pero no abarca de manera tan extensa el derecho a la intimidad o la protección de datos personales, dejando en evidencia que la legislación colombiana aún tiene un camino que recorrer en áreas y casos que se le escapan a la regulación actual. Por lo tanto, no puede considerarse una regulación exhaustiva y sistemática de los derechos que se encuentran en conexidad con el de habeas data.

Además de reiterar la trascendencia del consentimiento y la autorización del titular para que sus datos reposen en determinadas bases de datos, la sentencia destaca que, el hecho de que actualmente se pueda acumular infinidad de datos y hacerles a estos un “seguimiento en una memoria indefectible, de objetivizarlas y transmitirlas como mercancía en forma de cintas, rollos o discos magnéticos” implica una clase de poderío nuevo sobre el individuo, el poder informático. (Corte Constitucional de Colombia, Sentencia C-748, 2011).

Finalmente, respecto a la información que reposa en bases de datos como los sistemas de videovigilancia, la Corte expresa que, para que se configure una vulneración de datos la información contenida en el archivo debe haber sido recogida de manera ilegal, sin el consentimiento del titular del dato (i), ser errónea (ii) o recaer sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente (iii).” (Corte Constitucional de Colombia, Sentencia C-748, 2011).

Por otro lado, cuando se trata de la circulación de datos verdaderos en los que el titular hubiere autorizado su recolección y almacenamiento, en un principio, no configura una vulneración a un derecho fundamental (Corte Constitucional de Colombia, Sentencia C-748, 2011).

La autorización como factor vertebrador del tratamiento de datos

A lo largo de este trabajo se ha reiterado en varias ocasiones la importancia que tiene para el legislador la autorización por parte del titular de los datos. En este orden de ideas, para mayor claridad procederemos a definir qué se entiende por autorización y de qué maneras puede obtenerse.

En primer lugar, la autorización, según el artículo tercero de la Ley Estatutaria 1581 de 2012, se trata de “el consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales” (Ley 1581, 2012, art. 3). Adicionalmente, y de conformidad con lo señalado por la Superintendencia de Industria y Comercio, entidad encargada de velar por la protección de datos personales y el derecho al hábeas data, así como lo desarrollado por vía jurisprudencial, se entiende por "previo" que la autorización debe ser otorgada antes de la recolección del dato; "expreso" implica que no puede haber lugar a duda o ambigüedad, sino que debe ser claro e inequívoco; además, el titular debe ser informado sobre la finalidad y el uso que se le darán a los datos antes de otorgar su consentimiento.

De acuerdo con el artículo séptimo del Decreto 1377 de 2013, el consentimiento podrá ser dado de las siguientes maneras:

1. Por escrito.
2. De forma oral.
3. Mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca (Decreto 1377, 2013, art. 7).

Un ejemplo del primer caso es cuando el titular del dato acepta por escrito y firma un documento que informa sobre el tratamiento. En el segundo caso, de forma oral, puede darse cuando se otorga la autorización en medio de grabaciones de audio o video.

También el artículo octavo del decreto establece que debe haber prueba de la autorización: "Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos" (Decreto 1377, 2013, art. 8).

La autorización en el tratamiento de datos sensibles

La normativa aplicable al caso del tratamiento de datos sensibles es la contenida en el Decreto 1377 de 2013:

> **Artículo 6°. De la autorización para el Tratamiento de datos personales sensibles.** El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley. En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6° de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:
>
> 1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.
> 2. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso. Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles. (Decreto 1377, 2013, art. 6).

Del artículo contenido en la norma se concluye que, no solo basta con que el titular otorgue su autorización para el tratamiento, sino que se debe ser explícito al mencionarle que, de cualquier manera, no está obligado a darlo, así como especificar cuáles de los datos que se están recogiendo son de tipo sensible y el fin con el que se almacenan. En todo caso, la

realización de una actividad no puede estar condicionada a la autorización sobre el tratamiento de datos sensibles. El decreto paralelamente menciona que, el tratamiento de datos sensibles está prohibido, salvo las excepciones específicas mencionadas en la Ley 1581 de 2012, las cuales se citan a continuación:

> **Artículo 6. Tratamiento de datos sensibles.** Se prohíbe el Tratamiento de datos sensibles, excepto cuando:
>
> **a)** El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;
>
> **b)** El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos casos, serán los representantes legales deberán otorgar su autorización;
>
> **c)** El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros
>
> **d)** El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;
>
> **e)** El Tratamiento tenga una finalidad histórica, estadística o científica. (Decreto 1377, 2013, art. 6).

Teniendo de presente las excepciones a la prohibición del tratamiento de datos, se encuentra que los sistemas de video vigilancia recolectan datos en ámbitos públicos y semiprivados (trabajo), por lo que se enmarcan en el literal A, dependiendo del caso particular.

Principios que Gobiernan el tratamiento de datos

Resta por examinar algunos de los principios que, por jurisprudencia de la Corte Constitucional y la ley estatuaria del 2012, se han previsto como orientadores y fundamentales al momento de realizar el tratamiento de datos y que son importantes para analizar los aspectos de la “autorización” del titular del dato.

Principio de Libertad

El contenido del artículo cuarto de la Ley 1581 de 2012 establece que: “El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento” (Ley 1581, 2012, art. 4).

Este principio indica que el manejo de datos solo puede hacerse si existe una autorización anterior que lo faculte; su objetivo es prohibir la obtención, circulación y suministro de información de manera ilegal, es decir, sin respetar lo establecido en la norma, ya que esto implicaría la vulneración de un derecho fundamental. La Corte Constitucional ha sostenido desde 1995 en su Sentencia SU-082 que "los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular” (Corte Constitucional de Colombia, Sentencia SU-082, 1995).

Principio de finalidad

Ilustrado en el artículo cuarto literal b de la misma ley, establece que: *“*El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.” (Ley 1581, 2012, art. 4, Literal B).

Describe que no se puede recolectar información *“*porque sí”*,* si no que esta acción deberá responder a un fin mayor u objetivo específico, resultando indispensable para llevar

a cabo alguna labor, de tal forma que está prohibido recolectar datos sin la determinación especifica de lo que se hará con los mismos; esto aplica de igual manera a su uso, divulgación y suministro cuando sea para una finalidad diferente a la inicialmente explicada.

Principio de necesidad

La Corte Constitucional, en la Sentencia C-748 de 6 de octubre de 2011, de revisión de la Ley Estatutaria de 2012, menciona que “bajo el principio de necesidad se entiende que los datos deberán ser conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos.” (Corte Constitucional de Colombia, Sentencia C-748, 2011).

Este principio establece que los datos podrán ser almacenados únicamente durante el periodo de tiempo para el que fueron inicialmente solicitados; una vez cumplido ese periodo, deberán ser eliminados.

Datos sensibles

Como se había descrito al inicio del escrito, existen diferentes tipos de datos. Los datos sensibles, según la Ley Estatutaria de 2012, se definen como:

> Artículo 5º. Datos sensibles: Son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelan el origen étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos. (Ley 1581, 2012, art. 5).

La Corte Constitucional en su Sentencia C-1011 de 2008, manifiesta que "La información sensible es aquella ‘(...) relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político.” Cuando se hablan de estos aspectos, se refiere a una esfera totalmente intima, propia de la autodeterminación de un individuo y que es impenetrable, por lo tanto, no es susceptible de interferencia externa de manera arbitraria; se le garantiza al individuo la posibilidad de actuar dentro de esa esfera de manera totalmente libre, en donde la única limitación es el límite de los derechos del resto y el ordenamiento jurídico. (Corte Constitucional de Colombia, Sentencia C-1011, 2008).

A partir de los conceptos brindados por la ley y la Corte sobre datos sensibles, se puede encasillar a los sistemas de videovigilancia dentro de esta categoría, ya que los datos que recolectan permiten la identificación de las personas (titular del dato). Específicamente, se trata de datos biométricos, los cuales pueden afectar la vida e inclusive la dignidad de una persona.

Los datos biométricos son aquellos que permiten identificar a una persona física mediante procedimientos técnicos que recogen información sobre sus características físicas, corporales o conductuales. Esta información es considerada sensible, ya que a partir de los sistemas de video vigilancia se obtienen datos sobre el modo de caminar, la contextura, el comportamiento y la imagen física de una persona en movimiento.

Conclusión del segundo Informe

Se concluye que los sistemas de video vigilancia, al capturar la imagen de una persona (tratamiento), pueden identificar a esa persona de manera única (dato personal), y dicha información puede ser almacenada en una base de datos. Por lo tanto, el Derecho a la Protección de Datos Personales o a la intimidad está totalmente relacionado con los sistemas de video vigilancia, ya que se cumplen los dos elementos fundamentales: dato y tratamiento.

Cuando se trate de datos de carácter sensible siempre deberá mediar la autorización del titular de la información. Así mismo, el titular cuenta con la facultad de acceder a sus datos, conocerlos, rectificarlos e incluso pedir que sean retirados. Finalmente, en la vídeo vigilancia es totalmente aplicable la normativa de Ley Estatutaria 1581 de 2012, por lo que se deben observar y respetar los principios contenidos en la norma.

3.3. Análisis del derecho a la intimidad y habeas data frente al uso de sistemas de videovigilancia en el lugar de trabajo

Previamente analizados los elementos doctrinales en torno al debido proceso y proceso laboral disciplinario, así como la legislación colombiana en materia de datos sensibles y tratamiento de los mismos, en este informe se abordará la discusión de mayor tensión a la hora de resolver la pregunta problema de este trabajo de investigación de cara al vacío legal existente en Colombia sobre el uso de sistemas de videovigilancia en espacios de trabajo y en general en cualquier espacio, respetando el derecho a la intimidad pero garantizando el derecho al habeas data.

En la legislación colombiana el derecho al habeas data, está profundamente ligado con el de intimidad o también llamado protección de datos. Como se ha aludido anteriormente, se encuentran consagrados en el artículo 15 de la Constitución Política, lo que hace que al momento de analizar su aplicación o vulneración se haga en conjunto.

Empero, hay que dejar de presente que el habeas data hace referencia al derecho que tienen las personas a conocer y obtener su información almacenada en bases de datos, mientras que el derecho a la intimidad o protección de datos es una garantía que tienen los titulares de los datos almacenados sobre el respeto de su información frente a terceros e inclusive encargados del tratamiento de datos, es decir, el primer derecho está limitado por el segundo.

En concordancia con lo expresado, se destaca que el derecho al *habeas data* versa sobre la capacidad que tienen las personas para obtener su información privada y personal frente a terceros que la guarden en archivos. En este sentido, “quiere decir que la persona ya no es un sujeto pasivo frente a lo que pasa con sus datos; ahora tiene el derecho de saber cómo se recolectaron, para qué se van a utilizar, quién los tiene; si son erróneos o equívocos.” (Cervantes Díaz, 2009, p. 9).

Anudado lo anterior, el derecho a la intimidad o protección de datos es un derecho personalísimo que no puede ser invadido por interferencia de terceras personas. La Corte, mediante reiteración de jurisprudencia, lo define como “el espacio intangible, inmune a las intromisiones externas” del que deriva un “derecho a no ser forzado a escuchar o a ser lo que no desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto” (Corte Constitucional de Colombia, Sentencia T-552, 1997).

Entonces, ambos derechos, aunque íntimamente relacionados, pueden surgir situaciones en los que colisionen y se vean enfrentados, por lo que dependiendo de las particularidades del caso y lo dicho por la ley se determinará cual debe primar sobre el otro.

El respeto del derecho de la intimidad y habeas data en el trabajo

El sitio de trabajo resulta de especial atención, no solo porque sea la razón del trabajo, sino porque se trata de un sitio semiprivado, donde es muy normal el uso de los sistemas de video vigilancia por parte del empleador hacía sus empleados con fines de seguridad, protección del patrimonio de la empresa e inclusive para llevar un registro de que las funciones del cargo se estén realizando adecuadamente; ello amparado en la facultad de subordinación de la que está dotada el empleador explicada en el primer informe, aun así, vale la pena recordar que esta no puede ejercerse de manera absoluta.

En este orden de ideas, los derechos de intimidad y protección de datos, y su relación de tensión, cobran relevancia cuando se tratan de las relaciones laborales o patronales, puesto que el empleador intenta acceder a esferas que se podrían considerar íntimas del trabajador, de formas tales como la interceptación de conversaciones en redes sociales, uso de correos o sirviéndose de las cámaras de videovigilancia, dando como resultado que estos derechos puedan encontrarse en peligro de ser vulnerados, en especial cuando se graban ciertas situaciones dentro del ámbito laboral.

Hay que advertir que existen unos mínimos no negociables, que deben seguirse en aras de no vulnerar el derecho a la intimidad y habeas data de un trabajador. Primeramente, se deberá hacer conocer a los trabajadores de la existencia de los sistemas de video vigilancia en el sitio de trabajo y su ubicación, así como también, si se usan sistemas de control adicionales tales como la grabación de llamadas, y en general el manejo de los datos electrónicos entregados con ocasión a la relación laboral. Lo mencionado con el objetivo de establecer una relación laboral fundamentada en el consentimiento previo e informado, tal como lo dispone la ley estatutaria de protección de datos 1581 de 2012.

Aun así, lo anterior no implica una solución plena al límite del ejercicio de los derechos, puesto que ni siquiera el legislador ha reglamentado de manera específica la frontera entre uno y otro para el caso distintivo del ámbito laboral, lo que puede repercutir en actuaciones arbitrarias de parte del empleador y se estaría entonces, atenido a la aplicación de un test de proporcionalidad en cada coyuntura, lo que lleva a un problema aun mayor de criterio acerca los factores determinantes del test, de frente a la autoridad administrativa o judicial que disponga la aplicación de los criterios de necesidad, proporcionalidad e idoneidad de la medida.

Ciertamente, en el marco de una relación laboral los derechos a la intimidad y al *habeas data* indudablemente cuentan con un rango constitucional que los protege con inviolabilidad, sin embargo, “los espacios de trabajo al configurarse por varias personas se

convierten en entornos más sociables, en dónde implica la interacción con personas el cual conlleva al fortalecimiento de las relaciones sociales y obliga en cierta medida a las personas a salir de su esfera íntima” (Restrepo, 2020, p. 10).

La Corte en la sentencia C-602 de 2016 hace un contraste interesante sobre el derecho a la intimidad como un derecho “que busca ser salvaguardado por la inviolabilidad del domicilio, no es un valor puramente dicotómico, de tal manera que una actividad es estrictamente reservada o totalmente pública” demostrando que aunque en un principio se veía que no había punto medio entre estas, la experiencia social y humana ha demostrado que los individuos desarrollan una variedad inmensa de comportamientos que aunque pueden considerarse íntimos en ciertos aspectos, son públicos al mismo tiempo en otros; tal es el caso de las relaciones laborales, propone el siguiente ejemplo “es indudable que la vida familiar de una persona es un asunto más privado que sus relaciones de trabajo, pero eso no significa que su desempeño laboral sea una actividad pública que pueda automáticamente ser conocida y examinada por las autoridades y las demás personas.” Entonces podemos deducir acorde con lo dicho por jurisprudencia que, existen diferentes clases de esferas del ser humano y que dependiendo de cuál estemos analizando, tendrá un grado mayor de protección constitucional. (Corte Constitucional de Colombia, Sentencia C-602, 2016).

La perspectiva española (estudio de derecho comparado)

Aunque en Colombia aún existe un camino largo en cuanto a legislación sobre el uso de sistemas de videovigilancia se refiere, en el continente europeo por el contrario hay algo más de desarrollo en este tema, tal es el caso de España.

La legislación española en el Estatuto de los Trabajadores regula en su artículo 20 el uso de medidas y herramientas que se consideren necesarias para el control del correcto desarrollo de la actividad laboral. Dice así el texto español:

¨Artículo 20. Dirección y control de la actividad laboral.

(…)

3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad. ¨ (Estatuto laboral Español,1994)

A partir del texto citado se puede deducir que al permitir la adopción de las medidas que se consideren más *oportunas*, con el fin de a verificar el cumplimiento de las obligaciones y los deberes legales de los trabajadores, el derecho a la intimidad se torna flexible hasta cierto punto, con el fin de permitir que las empresas puedan verificar como se está llevando a cabo la operación encomendada a sus trabajadores a través del uso de sistemas de videovigilancia al que se refiere el artículo siguiente del mismo estatuto:

Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.

Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales. (Estatuto laboral Español,1994)

En el régimen español, también se ha analizado el aspecto de la licitud de la prueba contenida en una grabación como sustento para sancionar disciplinariamente en el ámbito laboral. En todo caso, la postura generalizada en este país, es que se puede considerar lícita dicha prueba siempre y cuando atienda al interés superior de la empresa de garantizar la seguridad en el espacio de trabajo; ello teniendo en cuenta que previamente, la persona

trabajadora hubiera conocido de la instalación de las cámaras y su ubicación por motivos de seguridad. Nos encontramos entonces ante un régimen normativo que abarca la posibilidad de supervisar actos ilícitos tanto de terceros como de los propios trabajadores. Sin embargo, no puede justificarse el uso de la "seguridad" como un motivo para estar controlando conductas estrictamente laborales, como ausencias en el puesto de trabajo, la productividad, o incluso las conversaciones que los empleados puedan tener entre ellos.

Para los españoles, el tema del consentimiento informado, o lo que en Colombia se llama “la autorización del titular del dato”, es un asunto relevante, aunque existen algunas diferencias, ya que la tesis del país europeo es un poco más permisiva que la nuestra; el régimen nacional español determina que en el marco de la relación laboral, no necesariamente se tiene que contar con el consentimiento previo del titular, en este caso el trabajo, previo a la recolección o captación de sus datos personales dice González Díaz (2020) que,

> El artículo 6.1 b) del RGPD señala que el tratamiento será válido, entre otras razones, cuando sea necesario ‘para la ejecución de un contrato en que el interesado es parte, una vez acordada su licitud’. Por otro, la LOPDGDD, en su artículo 6.2, especifica que ‘no será preciso el consentimiento cuando los datos se refieran a las partes de un contrato de una relación laboral y sean necesarios para su mantenimiento o cumplimiento’.” (González Díaz, 2020, p.25).

Esto quiere decir que hay una posibilidad autorizada por la ley de uso de cámaras de video vigilancia sin el requerimiento de haya mediado previamente una autorización expresa del trabajador, ello teniendo en cuenta las obligaciones y derechos que se adjudican tras la firma de un contrato de trabajo (González Díaz, 2020, p.25).

El uso de los sistemas de videovigilancia en el espacio de trabajo

Con relación al uso de sistemas de video vigilancia en el trabajo, dice la corte:

> la facultad de instalar mecanismos de vigilancia y control no puede ser ejercida de manera absoluta, aparejando una injerencia arbitraria en la esfera íntima de los trabajadores, y por tanto en eventos en los cuales se encuentren en pugna el derecho a la intimidad del trabajador y el derecho del empleador a dirigir su actividad laboral, se deberá determinar las circunstancias específicas del caso en concreto para ponderar los mismos en razón de la finalidad, proporcionalidad, necesidad e idoneidad de la medida, y por tanto determinar su razonabilidad, que deben encontrarse fundamentadas según el desarrollo inherente de la relación laboral. (Corte Constitucional de Colombia, Sentencia T-786, 2008)

De la sentencia de la Corte se puede rescatar que, evidentemente la instalación de cámaras de videovigilancia en el lugar de trabajo puede transgredir en parcialmente el derecho a la intimidad de los trabajadores, sin embargo, en muchas situaciones no se puede prescindir de ellas y resultan necesarias para el correcto desempeño de las funciones laborales, no obstante, siempre debe hacerse una ponderación de los derechos que se encuentran en juego, a partir de un análisis riguroso y razonable para determinar cuál deberá primar.

Respecto al ámbito objeto de discusión, la sentencia T-574 de 2017 se pronunció de la siguiente manera:

> El lugar de trabajo, en principio espacio semiprivado, no goza del mismo nivel de protección que el domicilio, debido a que el grado de privacidad es menor en atención a que allí tienen lugar actuaciones con repercusiones sociales significativas. Según las decisiones citadas, para establecer la violación del derecho a la intimidad es necesario considerar la expectativa que tiene el trabajador acerca de la confidencialidad de sus manifestaciones y, en ese sentido es necesario valorar, entre otras cosas, (i) si se trata de información íntima, sensible o que sólo le interesa a una

> persona en particular en atención al tipo de actividad que se desarrolle y (ii) si los empleados tienen o no conocimiento acerca del seguimiento de sus actividades. (Corte Constitucional de Colombia, Sentencia T-574, 2017).

Esta sentencia es bastante pertinente para efectos de la problemática concreta, dado que la propia Corte entiende que el lugar de trabajo es un espacio semiprivado, es decir, no se puede estar a la expectativa de que la intimidad individual gozará de la misma protección que pudiere tener en un espacio tal como el lugar de residencia.

Lo más importante en estas situaciones, es realmente que los trabajadores sepan de antemano de que están siendo grabados y monitoreados, y si dieron su autorización para ello; también se debe analizar si la grabación o dato que se está recolectando mediante el empleo de los sistemas video vigilancia, en ultimas solo le incumbe a la persona que es titular o si es de atención por parte del empleador, con relación a la función laboral encomendada al trabajador.

No obstante, el empleador en uso de la facultad de subordinación (concepto tratado en informes anteriores) no podrá en ningún caso ejercer un accionar que implique vulneración de derechos, por lo que estas problemáticas deberán seguir siendo resueltas por los magistrados de la Corte Constitucional, pues hoy en día, no existe una legislación que haya fijado esos alcances con límites y fronteras claras.

Concepto del Ministerio de trabajo

A lo largo del escrito se ha aludido a la falta de desarrollo legislativo en materia del uso de cámaras en espacios de trabajo, empero el 28 de junio de 2017 el Ministerio de Trabajo emitió el concepto 95992 para manifestarse al respecto; aunque no es una prerrogativa vinculante, brinda una visión que merece apreciación.

En el concepto, se responde la pregunta que formula una persona a la oficina asesora del Ministerio de Trabajo sobre si:

> “¿se pueden grabar las conversaciones de los celulares corporativos y los teléfonos corporativos y los correos electrónicos? ¿Para grabarlos debo notificarles que los voy a grabar? ¿Debe existir algún consentimiento del trabajador y qué sucede si el trabajador no acepta? ¿Es considerada práctica de acoso? ¿Las grabaciones, registros, información reclutada por estos medios de grabaciones de las empresas, así no sean consentidas por el trabajador, sirven como prueba para terminación del contrato?” (Ministerio de Trabajo, Concepto 95992, 2017).

La oficina asesora del Ministerio inicia señalando que a la fecha no hay como tal dentro de la normativa laboral de nuestro país, algo que regule la instalación de sistemas de video vigilancia en los espacios de trabajo, como tampoco el tema de la revisión de correos y celulares institucionales; con todo y esto, la ley no los ha catalogado como actos que sean legales o que vayan en contra de ella, por lo que acá no queda otro camino que hacer uso del conocido “principio de permisión”, que establece que todo aquello que no está prohibido, se encuentra permitido. Hace hincapié en que, si el empleador se va a beneficiar del principio de prohibición, en todo caso no podrá obviar “el respeto a la dignidad de la persona y siempre que no se viole el derecho a la intimidad y la privacidad del trabajador” (Ministerio de Trabajo, Concepto 95992, 2017).

Entonces, si se aplica el principio de permisión, las acciones que decida tomar el empleador no podrán contrariar el orden constitucional ni lo establecido en la normativa colombiana. En esta ocasión, la oficina jurídica recuerda el artículo 59 del Código Sustantivo del Trabajo:

> "Artículo 59. Prohibiciones a los Empleadores. Se prohíbe a los empleadores:

1. (…)
2. Ejecutar o autorizar cualquier acto que vulnere o restrinja los derechos de los trabajadores o que ofenda su dignidad" (Código Sustantivo del Trabajo de Colombia, 1950, art. 59).

Igualmente, se trata el tema del derecho a la intimidad del trabajador, rescatando el criterio de la Sentencia T-768 del 31 de julio de 2008, que establece el derecho a la intimidad como no absoluto y que puede ser sujeto de limitaciones o interferencias cuando se persigue un verdadero interés general, en el contexto de las relaciones laborales entre empleador y trabajador o entre compañeros de trabajo. En este orden de ideas, la magistrada ponente de la sentencia, la dra. Clara Inés Vargas, expone algunas ideas que resultan bastante interesantes en términos de dar claridad a las preguntas planteadas:

> a) Entre las intromisiones ilegítimas en el derecho a la intimidad por ocurrir en espacios que interesan exclusivamente al titular del derecho.
>
> b) Con aquellas donde las actividades interesan a la relación laboral o empresarial. Aquí debe reconocerse la potestad que tiene el empleador de dirección y organización de su empresa, indispensable para la buena marcha de la empresa o entidad, razón por la cual puede adoptar medidas orientadas al logro de sus objetivos.

Así pues, hay tres puntos importantes por analizar. Primeramente, las cámaras de video; sobre estas la Sala Plena de la Corte ha dicho que se pueden considerar una medida adecuada y justificada para uso del empleador, siempre que busque garantizar la protección de los intereses de la empresa, así como permitir una inspección del desempeño de las actividades laborales, por lo que si la medida se usa con estos fines se puede considerar “idónea y necesaria” (Corte Constitucional de Colombia, Sentencia T-768 de 2008).

El segundo punto corresponde al conocimiento del trabajador de la medida; dice la Corte que, si se van a hacer uso de sistemas de video vigilancia o similares, esta medida de seguridad debe ser primeramente conocida por el trabajador, ya que excepcionalmente su uso daría lugar a medidas subrepticias. (Corte Constitucional de Colombia, Sentencia T-768, 2008).

El último punto que menciona la Corte, refiere que está totalmente prohibido instalar cámaras “para la filmación de la vida íntima del empleado o trabajador, como en los lugares de servicios personales, o en los locales sindicales etc., con el fin exclusivo de filmar partes íntimas de la persona, o acosarla en el lugar del trabajo” puesto que configuraría a toda luz una vulneración total del derecho a la intimidad y dignidad, al ser una intromisión que no está permitida bajo ningún concepto (Corte Constitucional de Colombia, Sentencia T-768, 2008).

La oficina jurídica concluye expresando que, la instalación de cámaras de videovigilancia está permitida en el área de trabajo siempre y cuando esta actividad se encuentre fundamentada en el respeto a la dignidad del trabajador y en consonancia con sus derechos a la intimidad y privacidad. Ante el vacío legal en esta materia, refiere que puede acudirse al artículo 108 del Código Sustantivo del Trabajo, que enuncia que los reglamentos internos de trabajo deberán contener disposiciones normativas en puntos como los señalados en el numeral 10°, que dispone: " Prescripciones de orden y seguridad."

Finalmente entre otros temas tratados, la oficina asesora indica que el empleador puede instalar cámaras de videovigilancia si lo considera necesario, sin que ello represente una transgresión al derecho de intimidad, siempre y cuando “atiendan a las prescripciones de orden y seguridad establecidas en el Reglamento Interno de Trabajo, siempre que tales disposiciones respeten la honra, dignidad y la vida privada de sus trabajadores, (…) no es aceptable la implementación de disposiciones que desconozcan estos derechos” (Ministerio de Trabajo, Concepto 95992, 2017).

Guía Orientadora de la Superintendencia de Industria y Comercio

Ante la falta de una disposición normativa que regule el manejo de los sistemas de videovigilancia en relación con la protección de datos, en 2016 la Superintendencia de Industria y Comercio (SIC) como ente delegado para garantizar la protección de este derecho, expidió una guía dirigida a compañías y organizaciones que recolectan datos en calidad de Responsables o Encargados del Tratamiento de datos mediante cámaras, videocámaras, análogas o digitales, cámaras IP o mini-cámaras, y circuitos cerrados de televisión (CCTV).

La SIC establece que los encargados y responsables del tratamiento de datos deben observar las siguientes reglas en su actividad, cuyo cumplimiento estará sujeto a auditoría:

- Solicitar y conservar prueba de la autorización de los Titulares para el Tratamiento de sus datos personales.
- Implementar sistemas de videovigilancia solo cuando sea necesario para el cumplimiento de la finalidad propuesta, respetando la dignidad y demás derechos fundamentales de las personas.
- Limitar la recolección de imágenes a lo estrictamente necesario para cumplir el fin específico previamente concebido.
- Informar a los Titulares acerca de la recolección y demás formas de Tratamiento de las imágenes, así como la finalidad del mismo.
- Conservar las imágenes solo por el tiempo estrictamente necesario para cumplir con la finalidad del sistema de videovigilancia.
- Inscribir la base de datos que almacena las imágenes en el Registro Nacional de Bases de Datos, a menos que el Tratamiento consista únicamente en la reproducción o emisión de imágenes en tiempo real, sin perjuicio del cumplimiento de las demás disposiciones del Régimen General de Protección de Datos Personales.

- Suscribir cláusulas de confidencialidad con el personal que accederá a los sistemas de videovigilancia.
- No instalar sistemas de videovigilancia en lugares donde la recolección de imágenes, y en general, el Tratamiento de estos datos, pueda afectar la imagen o la vida privada e íntima de las personas. (SIC, Protección de datos personales en sistemas de videovigilancia, 2016).

Además, la SIC describe que los sistemas de videovigilancia y las bases de datos deben contar con medidas técnicas, humanas y administrativas que garanticen la seguridad de los datos almacenados, ya que se trata de datos personales y, por consiguiente, de información sensible. Estas medidas deben evitar la adulteración, pérdida, deterioro, consulta, uso o acceso no autorizado o fraudulento, con el fin de mantener la integridad de la información y respetar los derechos de sus titulares.

¿Qué dice la SIC sobre el acceso a las imágenes por parte de los Titulares de datos personales?

Conocer el punto de vista de la Superintendencia a este punto de la investigación resulta de ayuda en aras de resolver la pregunta problema planteada inicialmente. La SIC en el acápite noveno de la guía menciona que los titulares de los datos, están totalmente habilitados para solicitar el acceso de la información o datos que se almacenen sobre ellos, y que es un deber de los encargados y responsables del tratamiento adoptar las medidas que sean necesarias para proteger los derechos de los demás titulares de datos, cuyos datos personales también están siendo objeto de tratamiento (en el caso de las grabaciones de video vigilancia) junto con el titular que está solicitando el acceso. En adición, menciona que deben tenerse en cuenta los siguientes aspectos como medidas que pueden adoptarse:

• Establecer un procedimiento para acceder a las imágenes, que le permita a los Responsables y Encargados del Tratamiento verificar la calidad de Titular de quien solicita el acceso a la información.

• Requerir al Titular solicitante datos como fecha, hora, lugar, entre otros, para facilitar la ubicación de la imagen y limitar al máximo la exposición de imágenes de terceros.

• Si en la imagen aparece un (unos) tercero(s) Titular(es) de datos personales, se deberá contar con la autorización de dicho(s) tercero(s) para la entrega de la cinta o grabación.

• Si no se tiene la autorización de los terceros para divulgar la información contenida en la cinta o grabación requerida, los Responsables y Encargados del Tratamiento deben garantizar la anonimización del (los) dato (s) del (los) tercero (s), tomando medidas encaminadas a tal n, como hacer borrosa o fragmentar la imagen de dicho (s) tercero (s). (SIC, Protección de datos personales en sistemas de videovigilancia, 2016).

Finalmente, como recomendaciones generales a los encargados y responsables del tratamiento de datos para la elaboración y construcción de las políticas de acceso a los datos, se expresan estas:

• Evalúe el impacto que un SV puede tener respecto de la intimidad y la protección de los datos personales de los Titulares de información y determine si realmente necesita la implementación del mismo para lograr la finalidad perseguida.

• Determine y limite el período de tiempo que permanecerá la información en sus bases de datos teniendo en cuenta la finalidad para la cual se recolectó y documente la supresión de la misma.

• Obtenga la autorización o consentimiento del Titular de los datos personales para el Tratamiento de los mismos, adoptando los mecanismos necesarios para dar cumplimiento a lo establecido en el Régimen General de Protección de Datos Personales.

• Implemente medidas de seguridad y confidencialidad para el Tratamiento de la información recolectada mediante los SV.

• Diseñe políticas y protocolos para la recolección, uso, circulación, conservación y disposición final de la información que recolecta, así como para la atención de las peticiones, consultas y reclamos presentados por los Titulares e informe de estos al personal que opere los SV. (SIC, Protección de datos personales en sistemas de videovigilancia, 2016).

(…)”

Conclusión del tercer informe

Desafortunadamente no hay en Colombia actualmente un desarrollo jurídico claro y conciso en materia del uso de sistemas de video vigilancia en lugares de trabajo de cara a la protección de datos y derecho al habeas data, sin embargo, existen aproximaciones jurisprudenciales de sentencias de la corte y conceptuales de entidades oficiales que se pueden utilizar de manera orientadora tales como el Ministerio de Trabajo y la Superintendencia de industria y Comercio. En todo caso, se hace alusión que ante la falta de legislación deberán ser los empleadores los encargados de regular internamente en sus manuales el uso y alcance de los sistemas de video vigilancia, aplicando los test de proporcionalidad pertinentes en las situaciones en donde se vean enfrentados dos o más derechos, para elegir cuál deberá primar siendo observantes de las garantías consagradas en la constitución.

4. Propuesta de modificación al instructivo ISCP007 de “Servicios de Seguridad Electrónica” de Electrificadora de Santander S.A. E.S.P

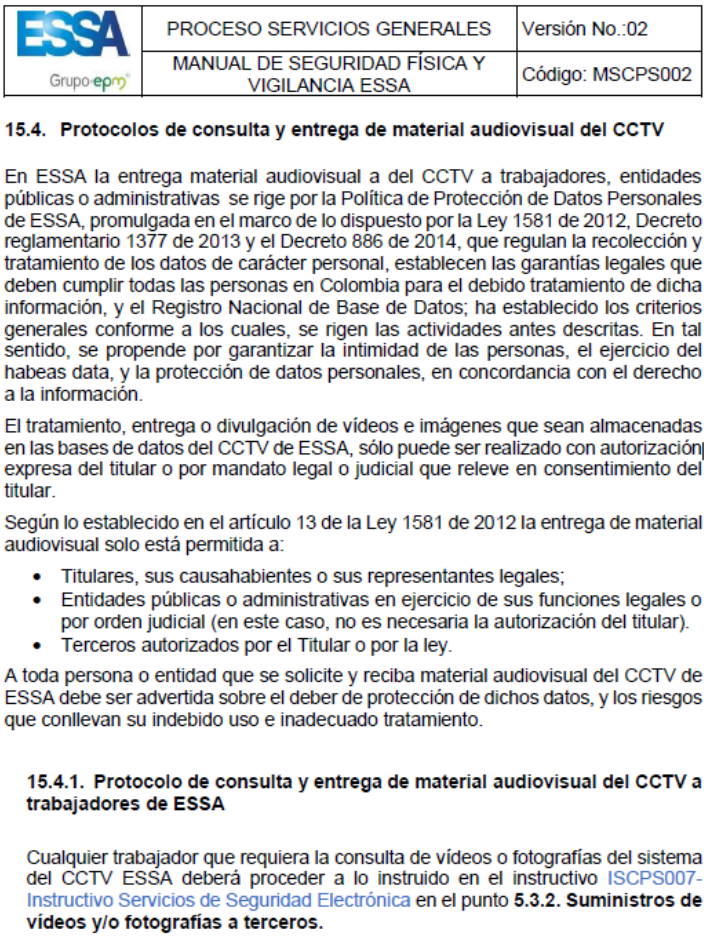
El manual de seguridad física y vigilancia de ESSA es el encargado de establecer el protocolo de consulta y entrega de material de CCTV a trabajadores de ESSA, entidades públicas o administrativas y se rige por la política de protección de datos personales de ESSA, promulgada en el marco de los dispuesto por la ley 1581 de 2012 y los decretos

reglamentarios 1377 de 2013 y el 866 de 2014, que regulan la recolección y tratamiento de datos de carácter personal y establecen las garantías legales que deben cumplir todas las personas en Colombia para el debido tratamiento de dicha información, y el Registro Nacional en la Base de datos.

En este manual se expresa, que solo se hará entrega o divulgación de videos e imágenes que sean almacenados en las bases de CCTV con autorización expresa del titular o por mandato legal o judicial. Así pues, para el procedimiento de entrega de datos indica que deberá procederse de conformidad a lo consignado en el instructivo ISCP007 de “Servicios de Seguridad Electrónica” en el punto 5.3.2 Suministros de vídeos y/o fotografías a terceros:

Figura 7.

Manual de seguridad física y vigilancia ESSA MSCPS002



ESSA Grupo epm	PROCESO SERVICIOS GENERALES	Versión No.:02
	MANUAL DE SEGURIDAD FÍSICA Y VIGILANCIA ESSA	Código: MSCPS002

15.4. Protocolos de consulta y entrega de material audiovisual del CCTV

En ESSA la entrega material audiovisual a del CCTV a trabajadores, entidades públicas o administrativas se rige por la Política de Protección de Datos Personales de ESSA, promulgada en el marco de lo dispuesto por la Ley 1581 de 2012, Decreto reglamentario 1377 de 2013 y el Decreto 886 de 2014, que regulan la recolección y tratamiento de los datos de carácter personal, establecen las garantías legales que deben cumplir todas las personas en Colombia para el debido tratamiento de dicha información, y el Registro Nacional de Base de Datos; ha establecido los criterios generales conforme a los cuales, se rigen las actividades antes descritas. En tal sentido, se propende por garantizar la intimidad de las personas, el ejercicio del habeas data, y la protección de datos personales, en concordancia con el derecho a la información.

El tratamiento, entrega o divulgación de vídeos e imágenes que sean almacenadas en las bases de datos del CCTV de ESSA, sólo puede ser realizado con autorización expresa del titular o por mandato legal o judicial que releve en consentimiento del titular.

Según lo establecido en el artículo 13 de la Ley 1581 de 2012 la entrega de material audiovisual solo está permitida a:

- Titulares, sus causahabientes o sus representantes legales;
- Entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial (en este caso, no es necesaria la autorización del titular).
- Terceros autorizados por el Titular o por la ley.

A toda persona o entidad que se solicite y reciba material audiovisual del CCTV de ESSA debe ser advertida sobre el deber de protección de dichos datos, y los riesgos que conllevan su indebido uso e inadecuado tratamiento.

15.4.1. Protocolo de consulta y entrega de material audiovisual del CCTV a trabajadores de ESSA

Cualquier trabajador que requiera la consulta de vídeos o fotografías del sistema del CCTV ESSA deberá proceder a lo instruido en el instructivo ISCPS007-Instructivo Servicios de Seguridad Electrónica en el punto **5.3.2. Suministros de vídeos y/o fotografías a terceros.**

Figura 8.

Instructivo ISCPS007servicios de seguridad electrónica

ESSA Grupo epm	MACROPROCESO PRESTACIÓN DE SERVICIOS CORPORATIVOS	Versión No.: 05
	PROCESO PRESTACIÓN DE SERVICIOS GENERALES	Página 4 de 8
	INSTRUCTIVO SERVICIOS DE SEGURIDAD ELECTRÓNICA	Código: ISCPS007

deben ser autorizadas por el profesional 3 - rol de Seguridad Física equipo de trabajo Gestión Logística y de Seguridad y debe quedar registrado en minuta.

5.3.2 Suministro de videos y/o fotografías a terceros:

Se procederá de acuerdo con la Política de Protección de Datos Personales de ESSA y al cumplimiento de la Ley 1581 del 2012, Decreto reglamentario 1377 de 2013 y el Decreto 886 de 2014.

Para efectuar la solicitud de acceso a un video y/o fotografía especifica, se establecen los siguientes alcances:

- Si dicha solicitud corresponde a una gestión de alcance interno para ESSA, deberá efectuarse la solicitud al buzón corporativo del profesional 3 - rol de Seguridad Física equipo de trabajo Gestión Logística y de Seguridad. Es importante precisar, que la solicitud deberá contener la autorización previa del jefe de área correspondiente que emite la solicitud. Una vez recibida la solicitud, el profesional 3 - rol de Seguridad Física equipo de trabajo Gestión Logística y de Seguridad escalará a la jefatura del Área de Suministro y Soporte Administrativo para su respectivo análisis y aprobación en caso de ser procedente.

- Si dicha solicitud corresponde a una gestión de alcance externo para ESSA, deberá asignarse al profesional 3 - rol de Seguridad Física equipo de trabajo Gestión Logística y de Seguridad, quien escalará a la jefatura del Área de Suministro y Soporte Administrativo para su respectivo análisis y aprobación en caso de ser procedente.

- Solamente para efectos del control, administración y seguimiento a la operación eléctrica, los operadores de monitoreo del CCTV ESSA, cuando detecten una novedad que ponga en riesgo la operación en las subestaciones monitoreadas, podrán compartir fotos y videos a el CDC en tiempo real para alertar o prevenir posibles accidentes o peligros, con el ingeniero jefe de turno del CDC.

El instructivo referenciado es el encargado de establecer los pasos a seguir para prestación del servicio de administración de sistemas de seguridad electrónica, con el fin de mejorar la calidad en la prestación de los servicios de vigilancia y seguridad privada, asegurando un adecuado nivel técnico y profesional.

No obstante, el acápite 5.3.2 del instructivo, es el único en la empresa que cuenta con una disposición respecto al suministro de fotos y videos contenidas en las cámaras de video vigilancia, y actualmente no es los suficientemente amplia en su contenido para cuando se trate de trabajadores de la empresa que quieran obtener copia del contenido de CCTV.

Así pues, se plantea la propuesta de modificación del instructivo incluyendo un acápite subsiguiente:

Suministro de videos y/o fotografías al personal cuando se trate de investigaciones disciplinarías

Se procederá de acuerdo con la política de protección de Datos Personales de ESSA y al cumplimiento de la ley 1581 de 2012 y los Decretos reglamentarios 1377 de 2013 y el Decreto 886 de 2014 y atendiendo a las prerrogativas de la Superintendencia de Industria y Comercio en materia de protección de datos personales en Sistemas de Video Vigilancia, así como jurisprudencia de la Corte Constitucional.

- Para determinar hacia donde se debe dirigir la solicitud, deberá tenerse en cuenta el alcance interno enunciado en el acápite anterior 5.3.2
- Solo podrá solicitar copia de las fotos y videos, el trabajador que demuestre la calidad de titular del dato, en los términos de la ley 1581 de 2012 o en ultimas el órgano disciplinario, valiéndose de la facultad sancionatoria derivada del elemento de subordinación, en los términos de la sentencia T574 de 2017.
- Solo se podrán solicitar copia de las fotos y/o videos de los últimos 3 meses.
- La solicitud deberá estar adecuadamente motivada, indicando fecha, hora y lugar de los videos, fotos y/o grabaciones que se requieren, expresando que su uso corresponde exclusivamente al trámite disciplinario que se adelanta y con la finalidad de ser aportada al proceso e incorporada al mismo como una prueba lícita en garantía de los derechos al debido proceso, defensa y contradicción.

- En caso de que concurran terceros en la grabación y no se cuente con la autorización de estos, en el material que se entregará estarán anonimizadas las caras de los terceros para proteger su intimidad.
- La información estará limitada únicamente a lo pertinente, en aras de reducir en lo posible la exposición de terceros.
- En ningún caso se suministrarán fotos y/o grabaciones en donde se vea comprometida de manera exponencial la imagen privada e íntima de las personas.
- La solicitud será estudiada por el Área de Suministro y soporte administrativo para determinar su procedencia, según las circunstancias específicas del caso

Conclusión informe final

La propuesta de modificación que se presenta en este informe final es el resultado del grueso de investigación legislativa y jurisprudencial que se recopiló en este trabajo, prestando especial atención a la ley 1581 de 2012 y sus decretos reglamentarios 1377 de 2013 y el Decreto 886 de 2014, apoyándose a su vez para su redacción, en la Guía para protección de datos en los sistemas de video vigilancia, expedida por la Superintendencia de Industria y Comercio en el año 2016.

5. Conclusiones

En el marco del apoyo jurídico al área de Asuntos Legales y Secretaría General, así como la ayuda asistiendo a la profesional del área Lida Mayerly López Pedraza en materia de derecho laboral relacionado con situaciones administrativas internas relacionadas con los trabajadores de Electrificadora de Santander S.A. E.S.P., se identificó que hasta la fecha existen inconvenientes con relación a los procesos disciplinarios laborales que adelanta el equipo de Administración de Personal, adscrito al Área de Servicios Corporativos, en lo relativo al suministro de grabaciones de video vigilancia contenidas en los CCTV de la empresa. El inconveniente radicaba en que muchas veces en estas grabaciones quedaban

consignadas las comisiones de conductas constitutivas de faltas disciplinarias y en razón a esto, quienes estaban siendo investigados solicitaban copia de este material, sin que se tuviese claro dentro del instructivo el procedimiento a seguir en estos casos para la entrega del mismo sin vulnerar los derechos a la intimidad de los demás trabajadores que aparecen en dichos registros audiovisuales por la instalación de las cámaras en los lugares de trabajo.

Luego del estudio realizado en este trabajo investigativo, se encontró que, respecto al tema del consentimiento y autorización del tratamiento de los datos, todos los trabajadores de ESSA al momento de vincularse formalmente con la empresa mediante la firma del contrato de trabajo, aceptan cláusulas que se encuentran contenidas en este y en donde se informa que van a estar siendo grabados y monitoreados por la empresa durante su jornada laboral. En este sentid, se puede determinar que se trata de un consentimiento previo, voluntario e informado, sobre la medida que adopta ESSA en función del ejercicio de su facultad de subordinación para supervisar el correcto funcionamiento de la empresa y velar por la seguridad en el espacio de trabajo. De igual manera, tras revisión se halló que la empresa cuenta con la señalización requerida por ley a lo largo de sus instalaciones, sobre el uso de cámaras de video vigilancia, es decir, todo el personal que allí labora está plenamente informado de la existencia de estos aparatos electrónicos. Así pues, no comporta una transgresión sustancial al derecho de la intimidad que se predica esencialmente del fuero privado del trabajador, ya que las oficinas y en general instalaciones de la empresa (se excluyen baños, vestidores y relacionados) son espacios de tipo semiprivado, lo que implica que los trabajadores puedan estar siendo grabados constantemente, en pro del interés general y bienestar de la empresa.

Por otro lado, se logró evidenciar que el derecho al habeas data en la legislación y jurisprudencia colombiana es uno de los que está mejor desarrollado, a diferencia del derecho de intimidad o protección de datos. Entiéndase el primero como el derecho fundamental que tienen todos los titulares cuyos datos están siendo objeto de tratamiento, de poder acceder, consultarlos y que les sean suministrados, así como solicitar correcciones y supresión de este, de ser errónea la información contenida en la base de datos. Aplicando esta disposición en el

contexto específico de ESSA, podemos concluir, que para el caso de los procesos disciplinarios que se adelanten, deberá primeramente hacerse un análisis diagnóstico de un test de proporcionalidad entre el derecho al habeas data y de intimidad, para determinar qué derecho deberá cobrar mayor valor, observándose en función de cual representa mayor bienestar general y seguridad en el lugar de trabajo; ello quiere decir, que debe estudiarse la particularidad de cada caso específico; no obstante se deberá propender la garantía del derecho al habeas data, debido a que la empresa tiene el deber de suministrar las grabaciones de video vigilancia cuando sea el titular quien las requiera, aún más cuando esta solicitud se de en el curso de una investigación disciplinaria de la que este sea parte y no hayan otros medios probatorios para demostrar la comisión o no de la conducta, ya que la negativa podría estar configurando un menoscabo a los principios generales orientadores del debido proceso en las actuaciones administrativas.

Finalmente, la conclusión de este trabajo de investigación corresponde a la materialización de la solución hallada, frente a la problemática inicial, siendo esta la propuesta de modificación del instructivo ISCPS007 “Servicios de seguridad Electrónica” con la inclusión del numeral “*5.3.3 Suministro de videos y/o fotografías al personal cuando se trate de investigaciones disciplinarías”,* en donde y por primera vez, se regla de manera específica y exegética el trámite para la entrega de material audiovisual con ocasión a uso en procesos disciplinarios; dicha reglamentación se construyó y redactó haciendo observancia de todas las disposiciones legales y garantías constitucionales existentes y vigentes actualmente, en aras de promover la tutela efectiva de los derechos de los trabajadores.

Referencias bibliograficas

Beltrán López, E. A. (2017). La protección de datos personales frente a los sistemas de vídeo vigilancia en Colombia. Recuperado de: http://hdl.handle.net/11396/5184.

Cervantes Díaz, F. (2009). Derecho a la intimidad y habeas data. *Derecho y Realidad*, 7(14), 179-198. Recuperado de: https://revistas.uptc.edu.co/index.php/derecho_realidad/article/download/5010/4087/.

Código Sustantivo del Trabajo [CST]. Decreto 2663 de 1950. Arts.111 y ss. agosto 5 de 1950 (Colombia)

Código Sustantivo del Trabajo [CST]. Decreto 2663 de 1950. Arts.59. agosto 5 de 1950 (Colombia)

Constitución Política de Colombia. [Const]. Art. 15. Julio 7 de 1991 (Colombia)

Constitución Política de Colombia. [Const]. Art. 29. Julio 7 de 1991 (Colombia)

Corte Constitucional de Colombia. (1996). *Sentencia T-301 de 1996*. Recuperado de: https://www.corteconstitucional.gov.co/relatoria/1996/T-301-96.htm.

Corte Constitucional de Colombia. (1997). *Sentencia T-552 de 1997*. Recuperado de: https://www.corteconstitucional.gov.co/relatoria/1997/T-552-97.htm.

Corte Constitucional de Colombia. (2000). *Sentencia C-386 de 2000*. Recuperado de: [URL si está disponible en línea].

Corte Constitucional de Colombia. (2002). *Sentencia T-537 de 2002*. Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2002/T-537-02.htm.

C**orte Constitucional de Colombia.** (2003). *Sentencia C-124 de 2003*. Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2003/C-124-03.htm.

Corte Constitucional de Colombia. (2004). *Sentencia C-934 de 2004*. Recuperado de: [URL si está disponible en línea].

Corte Constitucional de Colombia. (2005). *Sentencia C-822 de 2005*. Recuperado de: https://www.corteconstitucional.gov.co/relatoria/2005/C-822-05.htm.

Corte Constitucional de Colombia. (2014). *Sentencia C-593 de 2014*. Recuperado de: https://www.redjurista.com/Documents/corte_constitucional,_sentencia_de_control_de_constitucionalidad_no._593_de_2014.aspx.

Corte Suprema de Justicia de Colombia. (2006). *Sentencia 24668 del 6 de abril de 2006*. Recuperado de: Corte Suprema de Justicia, Sala de Casación Penal E. No. 24668 de 2006 - Colombia (redjurista.com)

Corte Suprema de Justicia de Colombia. (2006). *Sentencia 22179 del 9 de marzo de 2006*. Recuperado de: LEGIS Xperta | Plataforma digital con soluciones profesionales

Decreto 1377 de 2013 [Presidencia de la Republica]. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Junio 27 de 2013. Recuperado de: Decreto 1377 de 2013 - Gestor Normativo - Función Pública (funcionpublica.gov.co)

Gil Cifuentes, J. C. (2017). El debido proceso en la ley de habeas data. *CES Derecho*, 8(1), 191–204. Recuperado de: https://doi.org/10.21615/cesder.8.1.10.

González Díaz, F. A. (2020). Intimidad y protección de datos como derechos vertebradores en el uso de dispositivos de videovigilancia en el lugar de trabajo. *Revista De Trabajo Y Seguridad Social. CEF*, (451), 149–184. Recuperado de: https://doi.org/10.51302/rtss.2020.966.

Ley 1266 de 2008. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 47.123.

Ley 1581 de 2012. (2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587.

Restrepo, S. (2020). El alcance de la subordinación frente al derecho de la intimidad y al habeas data en un contrato laboral en Colombia. Recuperado de: http://hdl.handle.net/10554/47643.

Superintendencia de Industria y Comercio (SIC). (2016). *Protección de datos personales en sistemas de videovigilancia*. Recuperado de: https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Guia_Vigilancia_sept16_2016.pdf.

Tejada Correa, J. G. (2016). Debido proceso y procedimiento disciplinario laboral. *Opinión Jurídica*, 15(30), 227-248. Recuperado de: https://doi.org/10.22395/ojum.v15n30a11.